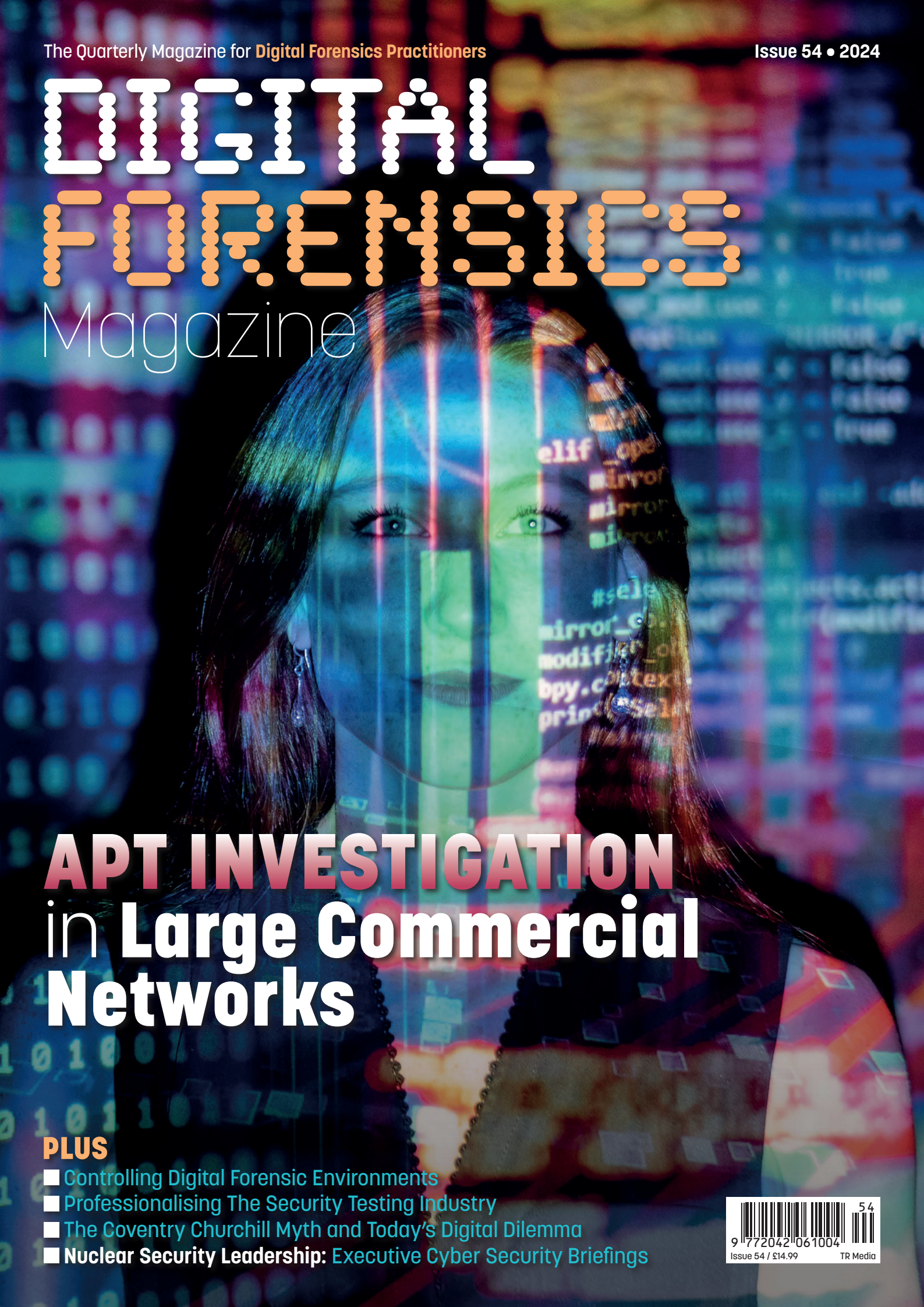
The Quarterly Magazine for Digital Forensics Practitioners

Issue 54 • 2024

DIGITAL FORENSICS Magazine



APT INVESTIGATION in Large Commercial Networks

PLUS

- Controlling Digital Forensic Environments
- Professionalising The Security Testing Industry
- The Coventry Churchill Myth and Today's Digital Dilemma
- **Nuclear Security Leadership:** Executive Cyber Security Briefings

54
9 772042 061004
Issue 54 / £14.99
TR Media

GLOBAL FORENSIC INVESTIGATION IN FOCUS

Forensics Europe Expo is the only international event covering every aspect of forensic investigation, making it the ideal meeting place for forensic solution providers and senior procurement personnel seeking to forge rewarding business partnerships.

If your products focus on Digital Forensic Investigation, Forensic Laboratory Equipment, Scene of Crime & Evidence Recovery or Forensic Analytics, Forensics Europe Expo 2024 will deliver a senior level procurement audience like no other conference or exhibition.

To add even more value, Forensics Europe Expo 2024 will be co-located with Counter Terror Expo (CTX). This co-location will enable delegates, visitors & exhibitors alike, the opportunity to seek relevant business synergies with a wider pool of security stakeholders attending CTX at our ExCel, London home in June.

Digital forensic investigation

Laboratory equipment

Scene of crime & evidence recovery

Forensic analytics

For exhibition and sponsorship enquires contact:
Rob Lozowski, rob@evendia.co +44(0)208 191 0981

Organised by: evendia

Supported by: Forensic Capability Network

Co-located with: CTX PROTECT • RESPOND • RECOVER

19-20 June 2024
ExCeL London

email: info@evendia.co | tel: +44 (0) 208 191 0981 | web: forensicseuropeexpo.com

Editorial

It has been a while since we released an issue and can only apologise and say thank you to those who have kept the faith. We have been in a holding pattern whilst we resolved some issues with the new website and challenges within the team. That being said we are now moving forward and planning the future with a high degree of optimism and lots of plans. The good news is that the price has been held yet again at our low price and we have no plans to increase the cost of subscription, indeed we have managed to trim costs such that we are able to invest in the magazine.

So what is in store for the future. Well, the new website is up and running and this will continue to develop and improve. If you do find any issues with the site, do let us know via the support ticketing system, such that we might get them resolved quickly. Within the revamp of the website, you will see we are trying out new 'News' and 'Blog Posting' formats, these are not yet settled as we want to find the optimum ways to deliver the news in a timely and meaningful manner. We have been looking at the various news sources we have access to and are getting close to establishing an automated process for up-to-date news content delivery.

Blog postings are in our terms "Short Form Articles", and we are looking to encourage those who have an article, but do not have the time or will to write a full article to contact us to discuss the ability to write and have your blogs posted. We will be putting up a webpage related to this shortly. It is fair to say that we get a fair amount of Blog Posts that are blatant advertising, and unless they are paid for adverts, these very rarely get through the editorial process. Where we do accept paid for advertising, we do our best to make sure it is relevant to the readership of the site.

We are also working with a small group of individuals, and we are close to publishing our first ever 'Podcast'. This is again a new venture for us here and is a joint venture where we are supporting a team who are looking at the more diverse aspects of our profession. The first series is about Neurodiversity and Cyber Security, and we are excited about this coming to fruition, it has been building for the last year and we are now so close to releasing the first episode of the series, so keep watching the website for details.

Lastly, we have seen an explosion in our social media platforms, especially our LinkedIn group that we have kept private. We have done this on purpose to ensure that the content posted to the group is not only relevant, but it stops you getting bombarded with adverts that have not been approved or agreed to.

As ever if you have an idea for an article that you would like to read or even write about, do get in touch, and discuss your ideas with us.

Roy Isbell

Digital Forensics Magazine *is a quarterly magazine, published by TR Media Ltd, registered in the UK.*
It can be viewed online at:
www.digitalforensicsmagazine.com

Editorial Board
Roy Isbell, Alastair Clement, Scott Zimmerman & Angus Marshall

Acquisitions
Roy Isbell & Scott Zimmerman

Editor-in-Chief
Roy Isbell FIET FBCS CITP

Production and Design
Matt Dettmar
www.magazinedesigner.co.uk

Contributing Authors
Matt Carver, Brian Cusack, Roy Isbell, Andy Jenkins, Emily Kinsella, Angus Marshall, Richard Piggi & Scott C. Zimmerman

Technical Reviewers
Prof. Tim Watson, Scott Zimmerman, Roy Isbell & Angus Marshall

Website
Designed by BluCreative.co.uk

Contact

Editorial
Contributions to the magazine are always welcome; if you are interested in writing for Digital Forensics Magazine or would like to be on our technical review panel, please email us:
editorial@digitalforensicsmagazine.com
Alternatively, you could telephone us on:
+44 (0) 8445 717 318

News
If you have an interesting news items that you'd like us to cover, please contact us on:
news@digitalforensicsmagazine.com

Advertising
If you are interested in advertising in Digital Forensics Magazine or would like a copy of our media kit, contact the marketing team on:
marketing@digitalforensicsmagazine.com

Subscriptions
For all subscription enquiries, please visit our website at www.digitalforensicsmagazines.com and click on subscriptions.
For institutional subscriptions please contact our marketing department on marketing@digitalforensicsmagazine.com

Feedback
Feedback or letters to the editor should be sent to 360@digitalforensicsmagazine.com

Digital Edition Provider
Digital Forensics Magazine uses ZMags for its Digital Editions, allowing the creation of carbon neutral publications.

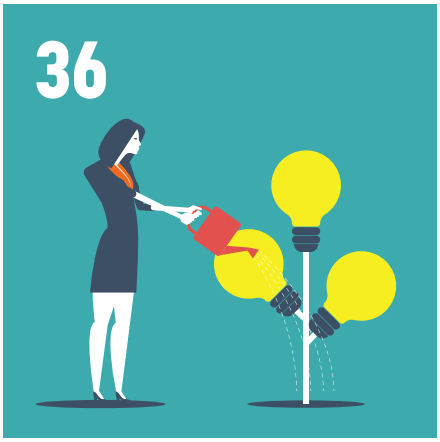
ALBERTO DANIEL HILL

OPERACION BITCOINS

THE STORY OF A HACKER

LOGIN TO HELL

Contents



FEATURES

REGULARS

LEGAL FEATURE
An Antitrust Case Against Google ***26***
Scott Zimmerman looks at how the United States Department of Justice (DoJ) is pursuing Google for monopolistic and antitrust activities.

APT INVESTIGATION in Large Commercial Networks

Brian Cusack invesgtigates Big Data methods.

Advanced Persistent Threats (APT) are dangerous and difficult to detect threats in any network and information system. Proactive defences may be implemented in the forms of threat intelligences and semantic deception strategies, but more commonly reactive defences are required to remediate the effects of APT security breaches. In this research the focus is on reactive investigation, and it sought to improve efficiencies for APT reactive investigation in large commercial networks. Large networks are characterised by large data volumes, data velocity, and veracity challenges. In these conditions attackers hide within the usual system workflows and conceal activities by using common network processes. Efficient data methods are required to identify sufficient evidence to satisfy investigation objectives. This involves leveraging the big data context for abstract design features that can ignore or triage the irrelevant from the relevant. Our contribution is to create a model to guide reactive APT investigation and then apply it to a Ransomware case study to demonstrate cost efficiencies. The core to the model is establishing evidential providence when so many similar activities occur in a network.

The identification challenge is distinguishing similar activities that may be unrelated to an APT attack, missing evidence trails deliberately erased by the APT, and semantic deceptions that frustrate Root cause analysis. The context for study is hence fraught with challenges. Deception, avoidance, and redaction have occurred before an investigator begins, and continue. Standard practice sets discovery around the four elements of network hardware, software, network, and users. Our contention is that more than standard practice is required to efficiently disclose APT activity in large commercial networks and that smarter tools are required to enhance investigation capability.

To initiate the research seventy-five 2014-2023 APT research articles published in the top six SCIMANGO Q1 security Journals were identified and analysed. It was found 80% of the publications concerned reactive research and 70% of these focused on APT detection methods. The literature weightings suggested proactive research into actors and threat intelligence were more difficult whereas reactive research works off the evidence left in networks after APT attack and has more tangible leads. Our key starting point was to define an APT from the original (1994) definition so that later variations could be benchmarked, and we could begin the evidential providence process by identifying exclusively APT evidence. Table 1 summarises and analyses the 1994 APT definition that is operationalised into an investigation model. ▷

FURTHER READING

Singh, S., Sharma, P., Moon, S, Moon, D. & Park, J. (2019). A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions. Journal of Supercomputing. 75,4543-4574

This article is a useful read and overview for APT research challenges. It provides an up-to-date review of APT network threats and the measures taken to defend from attack. The solutions are helpful reminders that APTs can be defeated.

Sharma A., Brij B. Gupta, B., Kumar, A., Singh, B. & Saraswat, V. (2022). Orchestration of APT malware evasive manoeuvers employed for eluding anti-virus and sandbox defense. Computers & Security. 115, 102627.

The APT deceives and evades network security measures by learning countermeasures. This article discloses techniques used for evasion and how antivirus defences are neutralised. Many APTs are fully automated and use AI methods to perform these tactics. It is an informative read and an alert to the uninformed.

Mookherjee, H., Theriault, A. & Wright, R. (2020). A baseline for unsupervised advanced persistent threat detection in system-level provenance. Future Generation Computer Systems. 108, 401-413.

The paper reports artificial intelligence (AI) application to APT behaviours to learn features for detection. The research is to establish a base line for trustworthy patterns of behaviour but also contributes AI method insight. Useful reading to get insight into how AI APT research is progressing.

Semantic Deception Attacks

Social engineering has popularised the network attack vector of semantic deception. A network is said to be made of hardware, software, and wetware. Semantic attacks attack the wetware or users to trick them into giving access to the network resources. The technical defences filter known threats but struggle to identify semantic attacks because technical usage is the same for all authorised users and the defects occur in the human mind not the technical system. Advances for detection using natural language and neural network technologies have some success, but these security features are not yet generally available or fully tested. The consequence is that any network has a serious vulnerability that education is attempting to patch. Semantic deception tricks the human mind into believing a falsehood that directs authorised and normal network use. Because the abstract intention is compromised then the net effect is network compromise and resource loss. We suggest in this article that defence must operate in a semantic protection layer that brokers the abstractions of security knowledge with the meaning of network context actions. In this way the intention and outcomes of actions may be forecasted and discriminated before impact. User education is a good start to wetware vulnerabilities but capability growth for artificial intelligence applications that function effectively in the sematic layer of network are also required.

APT CHARACTERISTIC	IDENTIFYING FEATURES		
	Abstraction	**Semantic**	**Attribute**
1. An adversary with sophisticated levels of expertise	*Competitive Warfare*	*Expert Intelligence*	*Reputation*
2 .An adversary with significant resources	*Enduring Capability*	*Strength*	*Numerical advantages*
3. Multiple different attack vectors (e.g., cyber, physical, and deception)	*Complex Identity*	*Multiplicity of co-ordinated attacks*	*Multi-factor impact*
4. Generate opportunities to achieve its objectives	*Innovates Success*	*Creative Methods*	*Vulnerability exploitation*
5. Establish and extend footholds within the information technology infrastructure	*Tactical Deployment*	*Permanent presence*	*Countable Occurrences*
6. Continually exfiltrating information	*Perpetual Action*	*Active agency*	*Services use*
7. Undermine or impede critical aspects of a mission, program, or organization	*Targeted Disruption*	*Goal & objective compromise*	*Successful failures*
8. Position for future action	*Strategic Deployment*	*Action ready*	*Concealment*
9. Pursues its objectives repeatedly over an extended period	*Timeless risk*	*Certain objective success*	*Event count*
10. Adapting to a defender's efforts to resist it	*Evasive learning*	*Avoids defences*	*State changes*
11. Determination to maintain the level of interaction needed to execute its objectives.	*Active state agent*	*Intentional network use*	*Transaction rates*

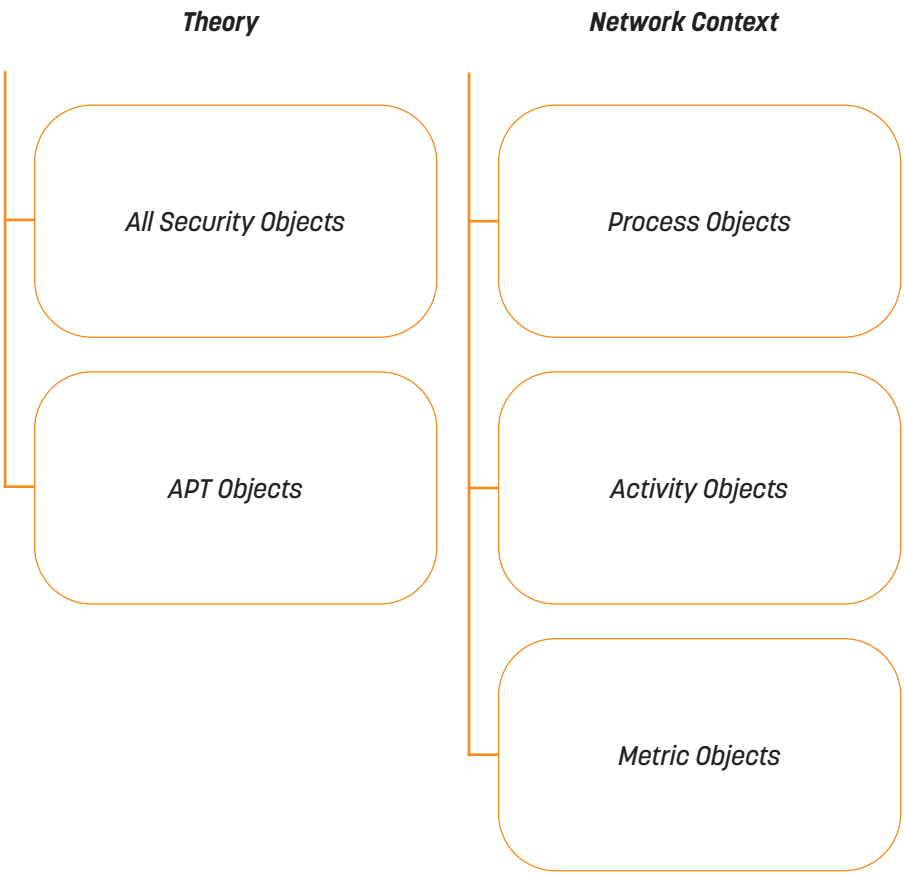
Table 1. APT Definition and Analysis

Learning From Past Research

Network security is divided in systems theory into a green trusted zone, a red untrusted zone, and a firewall boundary between the two zones to control traffic. The two zones fundamentally divide proactive research (Red), reactive research (Green), and the boundary is hybrid research. The success of APTs to penetrate network defences is acknowledged in all research reports, and the deliverable from the research is to develop a wide range of methods that restore the network state. Detection and discovery of APT activity in the network green zone is a common research theme in the literature reviewed. The research topics were artificial intelligence and deep learning for APT detection, traffic volume and exception analysis, behaviours monitoring, big data analysis, and APT lifecycle discovery processes. The limitation of each research project was scope. Table 1 lists and analyses the full scope of APT activity which is not fully covered in individual reports or the sum of the research reports. This reflects how academic research is done and the requirement to focus resources onto specific research targets. The gap in knowledge also means there are ample topics left for further research and the growth of APT security knowledge. The gap we spotted was that it is often not clear how the decision to discriminate APT traffic from other traffic in the network was determined. Most reports used pre-classified data that was researcher generated or downloaded from libraries, which is specifically cautioned against by other researchers. The result is that the advocated detection and classification methodologies may fail in different conditions and not give the intended security protections. We see these limitations and gaps in the literature as opportunities, and the unmet requirement for expanding the APT research agenda to be inclusive of all APT characteristics.

A summary of the research outcomes showed method development, and in particular methods for detecting APTs in a network Green Zone. Also, the description of tactical requirements for network defence featured as both security advice and guideline references. The analysis of network events for root causes identification was in few publications but network remediations to restore a stable state was a common theme. Several sophisticated methods for causal analysis of APT attacks using statistical and artificial intelligence appeared, and had the deliverable of security improvement steps, defensive awareness, and network readiness to resist attack. Discovery methods informed defensive strategy, tactics, and awareness of the threat. Traffic analysis research applied exception analysis to alert APT activity using big data methods. Other research focused on behaviours to propose defensive mechanisms that alert a network security function to disrupt the activity and to save the behavioural patterns for future reference. Again, we noted the research reports advance methods for network defence from APT attack but had big gaps in APT characteristic coverage, scrutiny for false positives, uncertainties in APT definition, and generalities that require more intense interrogation before effective countermeasures can be efficiently formulated.

Incident and event investigation is a key task for network security improvement. One reference argued that three domains of knowledge frame an effective APT investigation strategy. First, the APT ontology, second the general security domain knowledge, and third the network domain specific knowledge. These three domains of knowledge inform tactic and method for investigating and shape how



Model Class Selections

EXPERT TIP:
Get Expert APT Consultants

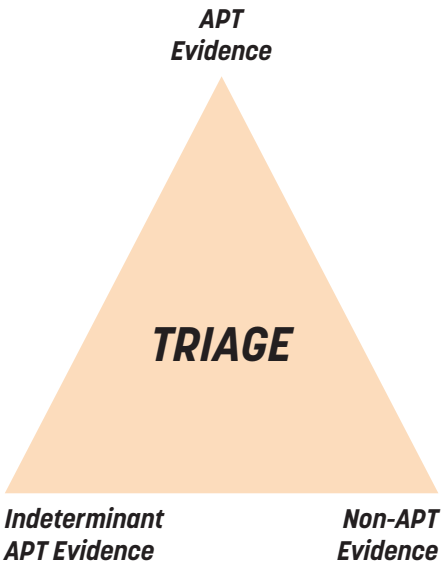
The size and scope of many network attacks today go beyond internal network security Unit capability to scope. The immediate attack effect can be remediated but the bigger picture of related threats may not be visible or tangible in terms of a full remediation requirement. An attack is an effect and root cause analysis should go beyond the immediate effect to match similar cases. However, a full investigation is costly for time, technical skill, and knowledge availability. APT attacks are global events initiated by well resourced and highly competent actors that hide from detection. Get outside help urgently. The cost of consultant fees is paid back rapidly in defence against further losses and restoration of normal work routines in the attacked network. Get APT specialist Consultants who have active knowledge of current global APT activities and regularly the monitor Dark Web for the trading that goes before and follows successful APT attacks.

evidence might be triaged for acceptance or rejection in an investigation. The target objects in APT investigation are static in stored data and live in traffic flows. The references scoped the many challenges an APT investigator faces and emphasised the challenges for evidential providence and trust in APT discovery processes. The impact of providence is for accurate and justified remedial advice. Admissibility for legal proceedings also requires satisfaction of criteria that relate to trust factors. To operationalise investigation Table 1 defines the object of interest in terms of descriptive behaviours but offers little objective framing for network APT investigation. Hence, the literature informs three domains of knowledge that must be reconciled and operationalised into an investigation framework. We chose to model the processes for process improvement, and to address the problem of providence in the APT context of multiple uncertainties and deception. We also defined a semantic discrimination mechanism to triage evidence and to provide potential cost efficiencies for investigation in large commercial networks. The following section reviews the APT forensic investigation model for reactive investigation design.

APT Forensic Investigation Model Design

The challenge for design is to bridge the theory and practice divide between the APT definition and the reality of a large functional commercial network. To structure the selection of classes for the APT investigation model The figure above groups security and network objects into theoretical and tangible categories, and then divides the categories into object classes. Evidential providence for APT attacks requires distinguishing APT evidence from other attacks and normal traffic in a network. Hence, an enhanced investigation model is to group classes of potential evidence, rank them, and deliver to investigation effectiveness and efficiencies. In this way the model has internal reliability checks, and external validity measures. The model classes logically flow from the set of all security abstractions, the abstract sub-class described by the APT definition, and the four elements of tangible network hardware, software, humans, and services. The four elements create the network service effect that has the primitive objects of network processes, network activities, and network metrics. Each process has many associated activities, and each activity has many metrics to measure network performances. Figure 1 represents the model structure with the abstract, logical, and physical selection of classes.

APT evidential providence is established by relationships between the classes. APT objects are a sub-class of all security objects and inherit definition and meaning from the parent class. However, the gap between theory and the tangible network context is polymorphic and introduces elements of uncertainty. Hence, there are many more security objects that inherit and use the Network Context objects and the related methods, than APT attacks. Therefore, we introduce a mediation layer termed the Semantic Layer to discriminate APT and non-APT evidence by meanings generated from the APT definition. The Semantic Layer is required to select evidence that satisfies the APT theoretical definition and to exclude evidence that has a polymorphic condition (The eight high level operational metrics are listed in Table 2). The risk is the exclusion of lower-level APT evidence when for example, the APT manages and uses other security objects for tactical advantage, and normal network traffic is also using the same methods. However, a network investigation is to identify what is clearly of APT attack origin so ▷



Semantic Discrimination Mechanism Triage of Evidence

APT-FIM METRIC	Y/N	EVIDENCE
Does the evidence show a permanent network presence?	Yes	Executed .exe file in system for at least 6 months. Fake user 3 months old in use.
Were the channels continually active?	Yes	At least 18 months. Multiple channels.
Have goals & objective targets failed?	Yes	Work system shut down. Payment system unusable.
Did strategic advantages materialize?	Yes	Information exfiltrated prior to ransomware. Calculated reputation loss.
Is there a timeline for the successful attack?	Yes	Multiple orchestrated incidents over 18 months.
Is there evidence of avoidance behaviours?	Yes	Anti-virus disabled or protective exclusions inserted to allow access and activities.
Is there evidence of intentional persistent behaviours?	Yes	Persistent remote login attempts. Multiple related attacks over 18 months.

Table 2. APT-FIM Metrics

that accurate and relevant remediation steps may be taken through security controls for APT risks. Hence, the figure above represents the three results possible from the semantic discrimination mechanism. Evidence may be non-polymorphic and accepted, polymorphic and assigned a trust probability P(), or rejected as non-APT. For efficiency the triage is to proceed in sequence from non-polymorphic evidence, polymorphic trust ranks, and to non-APT evidence. Once sufficient evidence is obtained to satisfy the investigation objectives the discovery process ceases.

Ransomware Case Example

The case study Public Agency served a general population of citizens and networked with the federal government information services system for citizen advice and transaction services in a large geographically dispersed service network. When employees logged onto their Public Services network a Ransomware demand screen appeared. The IT security Unit immediately escalated the attack to a security event as the whole network was impacted. The scale and impact on services required external consultants to investigate and to remediate the event. The consultants investigated and documented the Ransomware event, restored services, and provided detailed advice to defend future attacks, but the Public Agency wanted to know if this event was a one off or part of a larger orchestration of attacks on the network system. The APT forensic investigation model was applied to the secondary consultant data to determine evidence for an APT attack and if any specific APT network security remediation actions are required.

Semantic deception is used by attackers and defenders to disrupt mission targets.

The problem faced by the Public Agency after the successful remediation of the Ransomware attack is a common sense of trust violation and vulnerability. The attack impact was more than the material consequences and it also left doubts for staff and network users that more was to come. The problem faced was to decide if the Ransomware evidence and related causal factor analysis could be attributed to a more general and comprehensive attack on the network services. Prudent risk management required matching and mapping of the Ransomware Report with other previous incident and event reports to look for patterns. The forensic investigation model is designed for this work and to process large volumes of data efficiently for patterns fit to an APT attack. The APT attack profile is the most comprehensive and well documented big picture view network security can obtain. Other attack profiles map mechanisms and specific impacts but are weak on the big picture framing. Hence, the APT forensic investigation model can answer big picture questions and provide standardised advice to remediate a comprehensive set of network attacks. In this case, the application of the forensic investigation model to the Ransomware investigation Report was

Semantic Deception Learning

Attackers and defenders both learn from deception, the study of deception, and the investigation of what works in practice. An attacker often tries many ploys before breaking into a network and the resources. Each failed attempt provides a learning opportunity to improve and hone their craft. A defender places honey pots and monitors fake files in order to have the attacker disclose tactics, and to tire or deflect the intention of the attack. Learning in these senses is more than a stimulus reflex response loop. This type of learning is continuous, cognitive, and requires higher intelligences to succeed. Independent minds are making decisions for the next game move - play, pay, or exit. It is a highly intelligent game of competitive adversaries that apply any ploy available to succeed. An APT attacker is described as having a high level of intelligence and extensive resources, including time. The APT attacker plays a long game of deception, avoidance and learning to achieve the mission. The defender must play with the attacker to both learn behaviours but also to condition responses. The defender learns the attacker game to offer treats that satisfy the mission goal or make further progress too costly in terms of disclosure. Each proceeds without full knowledge of the other but with a game skill set that pivot toward an end game outcome - play, pay, or exit. Learning is a key element in understanding semantic deception and how it is used in many ways, and from many different perspectives to protect a network.

fast and efficient. The high-level model operational metrics were immediately applied to the secondary data sets to identify specific behaviours and target artefacts. The process of triage required no more than 10 minutes because Report evidence satisfied a positive assertion to each high-level operational metric, immediately signalling an APT event and no further action was needed to triage any further evidence. This was not the answer the Public Agency was looking for, but it alerted to certain future attacks, and gave time for readiness and to prepare countermeasures. The findings are documented in Table 2, and standardised advice for remediation and security policy review for APT events advised.

Discussion

The forensic investigation model was designed for reactive investigation in the network Green Zone. Hence, the first three Red Zone APT characteristics described in Table 1 are excluded from this model and research. Proactive Red Zone research is characterised by identification of the adversary, adversary resources, and threat intelligence for possible vectors of attack. These topics are out of scope for this research and fit another project. Further conceptual analysis for theoretical objects is required before improvements to the design can be made when the current design framework may not scope to theoretical objects and theoretical data.
The model primary discrimination is between morphic and polymorphic objects, and the secondary discrimination is a metric scale of trust probabilities. Feasibility analysis may show that an independent model design for proactive investigation requirements is effective, and then integration testing can proceed for comprehensive model improvement. There is further and ongoing research into the testing the model from other perspectives and other aspects of the APT security threat environment. For example, the semantic discrimination mechanism has not been pushed to its limits to disclose the capability to discriminate a wider range of semantic deceptions or to assign trust probabilities to polymorphic objects. The model is not yet tested on primary data for effectiveness and efficiency. These concerns remain for further research and model improvement.

The contribution of this research is to demonstrate in controlled conditions the capability of the forensic investigation model to enhance the efficiency and effectiveness of reactive network forensic APT investigation in large commercial networks. The model was tested on secondary data but theoretically it has similar efficiencies for primary data. Foremost the model looks for specific evidence that is equal to a morphic APT object and it processes this evidence first. An investigation can acquire sufficient evidence in this phase to end further discovery and to complete analysis for decision-making. In primary data the evidence field is much larger, but the same mechanism reduces the data volume to be processed and can stop an investigation once the first category of triage is satisfied. In large data sets if the first triage category is not satisfied then similarities associated with polymorphic objects require processing. Graduated scales of trust are used to select higher probabilities first, again reducing the amount of data required for processing.
A key resource in forensic investigation in big data contexts is time. The model prioritizes, ranks, and reduces the amount of evidence to be processed, and minimizes time to a decision. The embedded structure for evidential providence and root cause analysis determines the relationship of any evidence to the APT definition, lifting the confidence an investigator has in the process. A confident investigator makes decisive decisions, reduces activities, reduces time wastage, and has a trustworthy investigation outcome.

Conclusion

Semantic deception is used by attackers and defenders to disrupt mission targets, and to facilitate APT attacks. Forensic investigation of network security events can learn from both attacker and defender semantic deception ploys to gain proactive and reactive intelligence for situational awareness. In large commercial networks the challenge of large data volumes, data velocity, and veracity, demands that evidential providence can be established, and that investigations start with clear and manageable objectives that deliver sufficient representative evidence for decision-making. In this way causal analysis for remediation then applies the Pareto Principle to target only the ranked biggest causes or strongest coherent patterns, in the knowledge that smaller effects will redact. The forensic investigation model applies these principles to demonstrate investigation efficiencies, and effectiveness in big data contexts. The reactive context of study leaves further research to be done in proactive contexts, on primary data, and with tests so the model can be improved for automation. •

TOP FACT:

APT Success Features

The characteristics and features of an APT in the original definition (1984) suggest that success is more probable that failure when on attack. The key attributes of deception, intelligence, and unlimited resources such as time differentiate an APT attack from others. The APT uses many of the mechanisms of other attacks, the camouflage of big data, and the usual functional services of a network to achieve the mission aims. It differentiates from script-kiddies who have limited resources, one off attacks, and low-value targets attacks. An APT is focused on success, high returns, low disclosure, and often is untraceable and only known by the effects of a network attack.

REFERENCES

Auty, M. (2015). Anatomy of an advanced persistent threat. Network Security, 4, 13-16.
Chen, J., Su, C., Yeh, K. & Yung, M. (2018). Special Issue on Advanced Persistent Threat, Future Generation Computer Systems, 79(1), 243-246.
Huang, L. & Zhu, Q. (2020). A dynamic games approach to proactive defense strategies against Advanced Persistent Threats in cyber-physical systems. Computers & Security. 89, 101660.
Jafarian, J. & Niakanlahiji, A. (2023). MultiRHM: Defeating multi-staged enterprise intrusion attacks through multi-dimensional and multi-parameter host identity anonymization. Computers & Security. 124. 102958.
Joloudari, J., ... & Mosavic, A. (2020). Early Detection of the Advanced Persistent Threat Attack Using Performance Analysis of Deep Learning. IEEE ACCESS. 8, 186125-186137.
Khosravi, M. & Ladani, B. (2020). Alerts Correlation and Causal Analysis for APT Based Cyber Attack Detection. IEEE ACCESS, 8, 162642-162256.
Kida, M. & Olukoya, O. (2023). Nation-State Threat Actor Attribution Using Fuzzy Hashing. IEEE ACCESS. 11, 1148=1165.
Lajevardi, A. & Amini, M. (2019). A semantic-based correlation approach for detecting hybrid and low-level APTs. Future Generation Computer Systems, 96, 64-88.

Dr Brian Cusack *comes from a background of academic research in IS Security and IT Forensics. He currently directs the Cyber Forensic Research Centre NZ and is Adjunct Professor to the ECU Security Research Institute; and Professor at the Graduate Research Institute. He has been an International Standards Negotiator for over 20 years.*

@theOSPAs

Outstanding Security Performance Awards

Global OSPAs WINNERS

The 2024 Cyber OSPAs took place at Big SASIG in London on April 23rd, 2024. Hosted by the SASIG, the event recognised and rewarded outstanding performance in the cybersecurity sector, providing a platform to honour the industry's finest.

The winners of the 2024 Cyber OSPAs are:

Outstanding Chief Information Security Officer (CISO)

Sponsored by SASIG

Stuart Seymour – Virgin Media O2

Outstanding Cyber Security Professional

Dr. Ilia Kolochenko – ImmuniWeb

Outstanding Cyber Security Team

Global User Awareness – Allianz Group

Outstanding Cyber Security Consultant

DigitalXRAID

Outstanding Customer Service Initiative

POSSE App – Cyber Guardian

Outstanding Cyber Security Training / Awareness Initiative

CultureAI

Outstanding Cyber Security Partnership

Pervade and NPCC – Police CyberAlarm

Outstanding Police/Law Enforcement Initiative

Cyber Career Week – Police Scotland Cybercrime Harm Prevention Team

Outstanding Young Cyber Security Professional

Milind Purswani

Outstanding New Cyber Security Product

Sponsored by International Cyber Expo & National Cyber Security Show

Sophos Intercept X

Lifetime Achievement

Pat Ryan, CBE

Read the full announcement & winners' summaries at:

www.thecyberospas.com/2024/04/23/winners-announced-for-the-2024-cyber-ospas

The Coventry Churchill Myth and Today's Digital Dilemma

Andy Jenkinson separates Fact from Fiction.

History is often a complex tapestry of facts, interpretations, and sometimes, misconceptions. The bombing of Coventry during World War II and the alleged sacrifice of the city for intelligence reasons is one such myth. This article sheds light on the historical events surrounding the Coventry bombing and examines the contemporary concerns about government intelligence agencies and their actions in the digital realm which are known and simply exploited by adversaries.

The Coventry Bombing: A Historical Perspective

On the night of November 14, 1940, Coventry suffered a devastating bombing raid. Over 500 tons of explosives and 33,000 incendiary bombs were dropped by 300 German bombers. The devastating event has been the subject of much historical debate. One popular myth suggests that Winston Churchill had prior, specific knowledge of the attack upon Coventry and allowed it to happen to protect the secrecy of the Enigma code-breaking operation.

This assertion is not entirely accurate. Churchill received an Air Intelligence report on 12 November, just two days before the raid. That report listed five potential targets: Central London, Greater London, the Thames Valley, Kent, and Essex. Coventry was not specifically identified in the report. The decision-making processes were undoubtedly complex, and Churchill had to weigh the potential damage to civilian life against the strategic advantage of protecting Enigma intelligence. The myth of Coventry knowingly being sacrificed is an oversimplification of those decisions.

Digital Surveillance and Intelligence Agencies

Fast forward to the present day, and governments along with their Militaries and intelligence agencies have a new battleground, the digital realm. With the advent of the Internet, surveillance and intelligence-gathering became easier and more contentious. It's widely acknowledged that agencies like the NSA developed 'sophisticated' capabilities for monitoring and manipulating Internet Assets. These capabilities were initially developed with the aim of countering terrorist organisations and threats such as preventing another 9/11.

Surveillance exploiting Internet Assets is massive business. The agencies, undoubtedly led by the NSA, were tasked to lead that charge with hundreds of Operational Programmes such as PRISM and XKeyscore. The NSA collected data from numerous willing tech companies in the name of National Security. President Bush signed off tens, if not hundreds of $billions in the quest for Digital Supremacy and Dominance. Mistakes were unequivocally made. ▷

Churchill had to weigh the potential damage to civilian life against the strategic advantage of protecting Enigma intelligence.

Figure 1. Winston Churchill Visiting the Ruined Coventry Cathedral (www.goodfreephotos.com)

The Internet was an attractive area for the intelligence agencies to manipulate for surveillance due to its interoperability and ability to capture data on the fly and unknowingly redirect as desired enabling complete data capture, harvesting, and unprecedented analysis of data.

PRISM and XKeyscore were just two projects and powerful tools used by the United States' NSA to conduct mass surveillance and gather intelligence. Retrospectively these programs raised important questions about the balance between national security and individual privacy. A major oversight was the lax security of the infrastructure, the servers, and DNS which, if identified and exploited could enable mass exploitation by adversaries of the same date the NSA had collected. This became something of an Achilles Heel of the intelligence agencies and the Blueprint for cyber-crime.

PRISM was operated by the NSA under the legal authority of Section 702 of the Foreign Intelligence Surveillance Act (FISA). PRISM was first initiated in 2007 and grew into one of the NSA's primary data collection capabilities.

PRISM was primarily focused on collecting information from Internet-based communication services. Tech companies such as Google, Facebook, Microsoft, Apple, and others have been identified as participants in the PRISM program. These companies were compelled to provide the NSA with access to a wide range of user data, including emails, chat messages, photos, and videos. This data was then subjected to extensive analysis, enabling the NSA to track individuals, networks, and potential threats. Data security played second fiddle and was a secondary concern.

The revelation of PRISM raised significant privacy concerns worldwide. Critics argued that it infringed upon the Fourth Amendment rights of American citizens, which protect against unreasonable searches and seizures. Furthermore, the program was accused of overreach, as it collected vast amounts of data on both U.S. citizens and foreigners, often without specific targets or probable cause.

The legality of PRISM remains a subject of debate to this day. While the program operated under FISA, critics argued that the broad collection of data violated individual rights. Furthermore, the secret nature of the program raised questions about its accountability and oversight, especially regarding the potential for misuse.

Proponents of PRISM contended that it was essential for national security, allowing intelligence agencies to monitor and thwart potential terrorist threats. However, the revelation of PRISM by Edward Snowden sparked international outrage and strained diplomatic relations between the U.S. and its allies. The "Snowden Effect" also ignited a global debate on the trade-off between security and privacy.

Unlike PRISM, XKeyscore was not a data collection program in itself. Instead acted as an analytical tool that allowed analysts to search and filter vast amounts of data collected by the NSA. Analysts used XKeyscore to search for specific keywords, IP addresses, email addresses, and other criteria to identify potential threats or intelligence targets. XKeyscore provided a wide range of tools for tracking individuals, monitoring communications, and discovering patterns in data.

The Snowden revelations subjected XKeyscore, PRISM, and many other intelligence agencies programmes to face global criticism regarding the potential to infringe on privacy rights. The program's ability to perform detailed searches on vast amounts of data led to concerns about the collection and retention of personal information.

The legal and ethical concerns related to XKeyscore are similar to those of PRISM. Critics argued that the program lacked adequate oversight and transparency, allowing it to be misused or used against individuals who are not security threats. These concerns are as relevant today as they were in 2013 if not more so as not one, but two cyber wars rage in Ukraine and Israel.

Proponents of XKeyscore argued that it was a crucial tool for identifying and tracking individuals and organizations engaged in criminal or terrorist activities. The program was seen as a vital component of the U.S. government's counterterrorism efforts especially given the atrocities of the Twin Towers attack on September 11, 2001. That attack was still very fresh in the minds of the intelligence agencies and U.S. public. It still is to this day.

Ongoing debates surround PRISM, XKeyscore, and their latter-day programmes underscore the delicate balance between safeguarding individual privacy and ensuring national security. Striking the right balance is a challenging task, as too much emphasis on security can infringe on personal freedoms, while too much focus on privacy may hinder intelligence agencies' ability to protect the nation.

PRISM

The PRISM Intelligence Gathering Program was a clandestine surveillance program operated by the United States National Security Agency (NSA). It involved the collection of private electronic data from major internet companies such as Google, Facebook, Apple, Microsoft, and others. The program came to public attention in 2013 when classified documents were leaked by Edward Snowden, a former NSA contractor.

PRISM reportedly allowed the NSA to access vast amounts of user data including emails, chat logs, photos, videos, and other personal information. The program operated under the authority of Section 702 of the Foreign Intelligence Surveillance Act (FISA), which permits the targeting of non-U.S. persons located outside the United States for foreign intelligence purposes.

The revelations about the PRISM program sparked widespread controversy and debate about privacy rights, government surveillance, and the balance between national security and civil liberties. Critics argued that the program represented an overreach of government surveillance powers and raised concerns about the potential for abuse and the lack of transparency surrounding such programs.

The digital age has seen a near complete erosion of security, privacy, and civil liberties in the name of Surveillance.

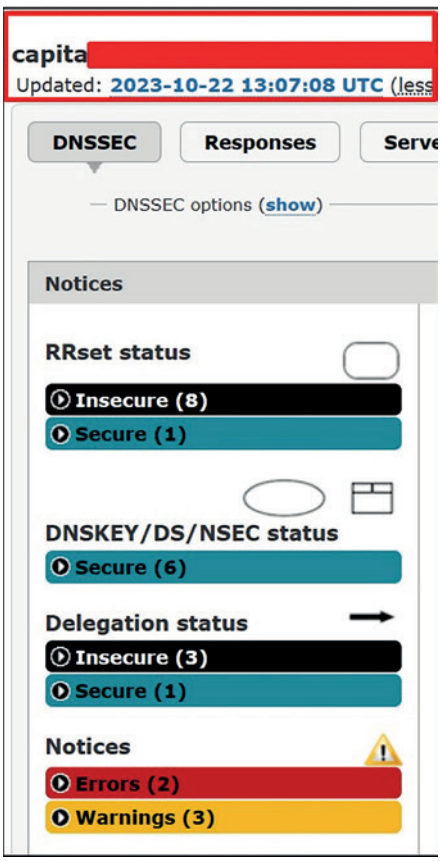


Figure 2. Whitethorn Capita Scan

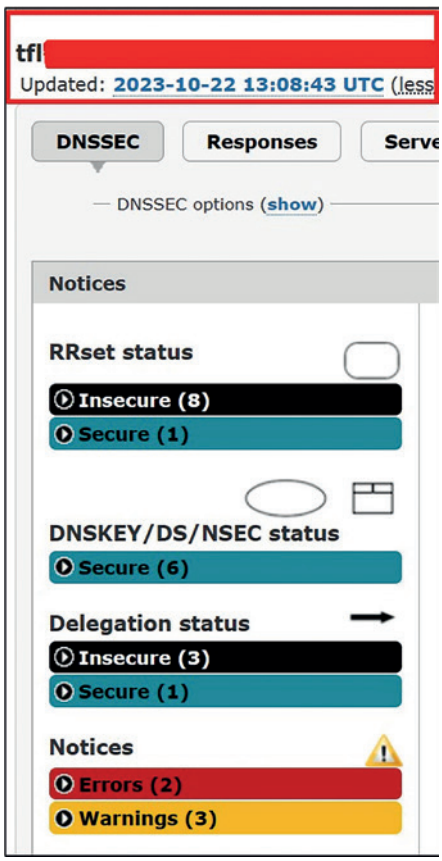


Figure 3. Whitethorn Scan

Edward Snowden's revelations back in 2013 confirmed exactly how invasive and comprehensive the surveillance capability was. Much of it with questionable legality. From 2013 to date, just a short decade, Cyber Crime and Cyber War has proliferated exponentially as our adversaries learnt and emulated the very same tactics and methods of exploitation that abuses exposed, insecure Internet Assets due to poor controls, management, and ignorance. Cyber Criminals and Nation States' Modus Operandi and Techniques are identical to that of the NSA and their counterparts. However, now not for global surveillance, but for global cybercrime, and Cyber War.

Let's consider a relatively recent technical based initiative here in the UK that highlights the potential for mass digital surveillance and manipulation. The Ultra-Low Emission Zone (ULEZ) that has recently been extended to now include all London Boroughs. ULEZ enjoyed revenues of £224, 633 in 2022 prior to the extension. This figure will increase substantially.

ULEZ works by capturing real time data of every vehicle within London that travels any distance by utilising one of thousands of cameras. The data collection is analysed against numerous databases including DVLA and VCA and uses an algorithm to determine if a vehicle is subject to a fee under the ULEZ scheme. Because the vehicle details are analysed against DVLA, the Personal Identifiable Information (PII) is retained and if a fee is to be levied, or non-payment pursued, the stored PII data can be utilised.

The commerciality and simplicity of this scheme is brought into question when one researches and analyses the basic Internet Assets and security failings of Capita, the outsourced third party who manages ULEZ along with the UK's Television Licence fees, NHS, and many other government programmes, along with The Transport for London's' own security failings.

In March 2023 Capita suffered a major Cyber Attack that has so far been confirmed to have cost Capita £25 million. More importantly, as the below real time examples of Capita and TFL's critical Domain Name System (DNS) demonstrate, both are totally exposed to Digital Intrusion, Data exfiltration, and further cyber incidents.

Capita and TFL collect, collate, and harvest PII data without ensuring basic security or best practice is adhered too despite having suffered a major cyber incident only months earlier. ▷

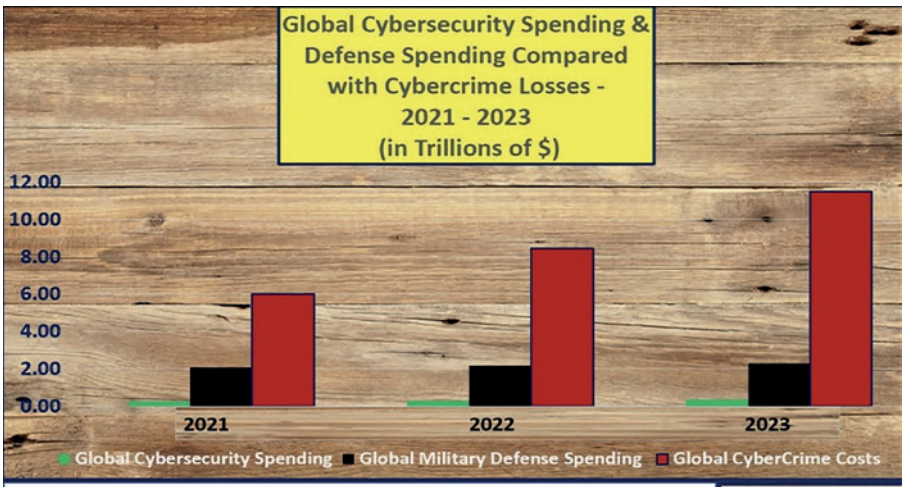
XKeyscore

The XKeyscore Intelligence Gathering Program is another clandestine surveillance program operated by the United States National Security Agency (NSA). It was revealed to the public through documents leaked by Edward Snowden in 2013, along with the PRISM program and other surveillance initiatives.

XKeyscore is a system that allows NSA analysts to search and analyse vast amounts of internet data, including emails, online chats, browsing histories, and other online activities, without obtaining prior authorization or a warrant. It's designed to provide real-time intelligence on targets of interest to the NSA.

One of the notable aspects of XKeyscore is its wide-reaching capability, allowing NSA analysts to search not only for specific individuals but also for patterns and behaviours that may indicate potential threats or targets for further surveillance. This program raised significant concerns about the scope of government surveillance and the potential for abuse of power.

Critics argue that the XKeyscore program, along with other NSA surveillance efforts, represents a significant intrusion into the privacy of individuals both within and outside the United States. They have raised questions about the legality, constitutionality, and ethics of such widespread surveillance practices.



Trillions (10^{12})

Year	2021	2022	2023
Combined GDP	96.30	100.20	105.00
Global Cybersecurity Spending	0.26	0.30	0.35
Global Defense Spending	2.10	2.18	2.30
Global Cyber Crime Costs	5.99	8.44	11.50

Figure 4. Cybersecurity Financial Comparison

Such failure places all the PII data collected at serious risk of being tampered with, abused, and exploited. A similar fate impacted the Electoral Commission when on the 8 August 2023 the Commission announced some 40 million UK Citizens data had been stolen due to Exchange Server issues.

The Electoral Commission stated that the NSCC assisted them in October 2022 when it was discovered a cyber-attack had been unknown for some 14 months that had started in August 2021. Figures 2 and 3 are screenshots of Whitethorn scans of Capita and TFL websites, they are identical due to using the same third party exposed, vulnerable, and insecure DNS servers. This insecurity enforces all data to be insecure and exposed. This also demonstrates a failure of regulatory requirements of UKDPA and GDPR and compliance.

In November 1940, Churchill was faced with ongoing genocide under the thick fog of war whilst an abhorrent enemy murdered millions of people. Ultimately his decisions and actions defeated Hitler and our enemies. His decisions were certainly difficult, yet 'We won the War' is testimony to those hard, often seemingly impossible decisions Churchill had to make under immense duress.

The NSA and their allies undoubtedly also have to make some tough decisions. The main difference is their original manipulation and abuse of the Internet has been turned against every citizen of the world that plays on the continued, forced ignorance of their citizens. What makes this all the more impactful and unpalatable is the NSA and their allies chose to keep everyone in the dark of their exposure and how to secure them whilst actively exploiting them. This is still very much the case hence the deficit of knowledge in certain Internet Asset security specifically DNS Servers.

Major concerns arose when these 'Highly Confidential' capabilities, intended only for national security purposes started to be used and exploited by our adversaries for nefarious purposes to infringe upon the security, privacy, and rights of organizations and citizens. The digital age has seen a near complete erosion of security, privacy, and civil liberties in the name of Surveillance. Many government agencies gain unfettered access to vast amounts of personal data without public consent that morphed into the Blueprint for Cyber Crime. To put this into perspective today cybercrime costs are a multiple of 5 times that of the annual U.S. Defence budget.

Edward Snowden

Edward Snowden is a former United States intelligence contractor who gained international fame for leaking highly classified information from the National Security Agency (NSA) in 2013. Born on June 21, 1983, in Elizabeth City, North Carolina, Snowden worked for various government contractors, including Dell and Booz Allen Hamilton, where he had access to sensitive information related to NSA surveillance programs.

In June 2013, Snowden made headlines around the world when he leaked a trove of classified documents to journalists, primarily Glenn Greenwald and Laura Poitras, revealing the extensive surveillance activities conducted by the NSA, including the PRISM and XKeyscore programs. These leaks exposed the widespread collection of electronic communications data, both domestically and internationally, by the US government.

Snowden's actions sparked intense debate about government surveillance, privacy rights, and the balance between national security and civil liberties. Some viewed him as a whistle-blower and a hero for exposing what they saw as unlawful and unconstitutional activities, while others criticized him for compromising national security and violating his oath of secrecy.

Following the leaks, Snowden fled the United States to avoid prosecution and sought asylum in various countries. In 2013, he received temporary asylum in Russia, where he remains as of my last update in January 2022. His actions continue to provoke discussions about surveillance, privacy, and government transparency around the world.

Cyber Crime and Cyber War has proliferated exponentially as our adversaries learnt and emulated the very same tactics and methods of exploitation that abuses exposed.

The Digital Dilemma

The digital era has brought to light a completely different kind of chaos. One that concerns the potential abuse of power by intelligence agencies and the subsequent utilization by Nation States for modern warfare as we have witnessed over the last two years. Hybrid Warfare is the intensity and barrage of Cyber Attacks that precede traditional Kinetic War. Some call this "Cyber War." No matter the term used, such attacks have a devastating effective in crippling an adversary's access to critical information and incapacitating most critical resources that are connected to the Internet. While the aim of intelligence agencies is to protect the nation from harm, it often appears that the same agencies are willing to overlook and compromise the rights, freedom, and overall security of their own citizens. Data capturing, collation, and harvesting makes an attractive target which can lead to total catastrophic impact to critical infrastructure and all due to basic digital security oversight and errors.

In recent years, there have been thousands of attacks, massive coverage, and revelations of mass data collection and surveillance programs, data breaches, and privacy violations. These actions have raised concerns about the imbalance between national security and individual liberties. The pervasive nature of digital surveillance is akin to watching organizations and individuals without their knowledge, raising serious ethical, moral, and legal questions.

Our adversaries now have identical capability and are not afraid to exploit unknown exposed positions. As the Director of the National Security Agency (NSA), General Paul Nakasone said, ''Our adversaries now have the same capability. They no longer fear us.''

The Coventry – Churchill myth highlights the complexity of historical events and the oversimplification of facts that can occur over time. The Capita and TFL basic security failings highlight continued basic security failings and ignorance with massive implications.

Undoubtedly in the digital age, we face a markedly different set of challenges to those Churchill faced. The rapid advancement of technology has given our intelligence agencies powerful tools, however, the responsibility to use, protect, and above all else, secure these tools along with the data they collect is crucial. Equally, knowledge-sharing to enable organizations, governments, and military to secure and protect them is paramount.

Vigilance, transparency, and accountability are necessary to ensure that the actions of intelligence agencies are just, lawful, and in the best interests of the people they are charged with protection. As we have witnessed on numerous occasions, that has not always been the case. Security of Internet Assets' exposed positions that can be exploited by the intelligence agencies, can also be exploited by everyone else, and are. •

REFERENCES

1. Coventry: What Really Happened - International Churchill Society (winstonchurchill.org) https://winstonchurchill.org/resources/myths/coventry-what-really-happened/

2. Capita Breach Costs - https://www.theguardian.com/business/2023/aug/04/cyber-attack-to-cost-outsourcing-firm-capita-up-to-25m

3. Electoral Commission hack exposed data of 40 million UK voters - https://techcrunch.com/2023/08/08/electoral-commission-hack-40-million-uk-voters/

Andy Jenkinson *is a seasoned business leader with 25 years' experience as a hands on CEO/COS coach and leader. A 'big deal' maker and business builder involved in many transactions over £100M. Advised business owners and created his own businesses within the technical, risk and compliance management markets. A thought provoking, challenging consummate professional and natural leader whose drive, energy and enthusiasm is not only infectious but inspirational ensuring everyone climbs the 'ladder of success' as a group.*

LEGAL Editorial

Elsewhere in this issue, curious readers can look at the antitrust case against Google which is currently in progress. Antitrust is a specific type of legal situation, and while I wouldn't want to spoil anything by divulging too much here, the term trust carries with it certain connotations. Here in the Legal News section, we have covered many types of stories: data breaches, crimes, strange technical events, and so forth, and one of those crime categories is directly related to a different kind of trust. Specifically, it involved individuals who were sending fraudulent invoices to large companies like Microsoft and Oracle. The perpetrators were apparently hoping those companies' Accounts Payable (AP) personnel would be too busy to vet the invoices properly, and would simply pay them. To put it another way, the perpetrators hoped that the AP personnel would trust the invoices were legitimate and treat them accordingly. For example, one individual billed for non-existent computers; he was caught, which is how we were able to read about him, but the idea was that the invoices were for fictional goods or services.

That type of fraud is rather clearly identified, at least in the common English definition of the word: asking for money for items, software, and/or services which were never provided – and were never intended to be provided – is a straightforward example. It is useful to mention intent here because that separates this topic from, say, a transaction in which the seller's facility burned down after payment was made but before delivery could occur: the seller likely intended to deliver on the purchase but was unable to do so due to exigent circumstances.

That differentiation started me thinking about trust from a different angle: what if someone sent an invoice to a company and (for example) asked for £30,000 but did not state any kind of purpose? As we have seen in the example above, if someone sends an invoice for the purchase of non-existent computers, that is clearly fraud because no computers would ever be delivered. To shed some light on the idea, let us examine the formal definition of fraud; for this we will be using our traditional reference of Black's Law Dictionary, Deluxe Tenth Edition:

Fraud 1. A Knowing misrepresentation or knowing concealment of a material fact made to induce another to act to his or her detriment. Fraud is usu. a tort, but in some cases (esp. when the conduct is willful) it may be a crime.

Actual Fraud. A concealment or false representation through an intentional or reckless statement or conduct that injures another who relies on it in acting.

There are a few dozen specific types of fraud, most of which are not germane to our discussion. However, I included the "actual fraud" as a secondary definition because it neatly reinforces a couple of points that are included in many of the definitions of the various types of fraud: there must be intentional (or knowing) misrepresentation that leads to a negative effect on the target. Essentially the perpetrator must be trying to gain an advantage through lying, including through lies of omission. For example, someone who is selling a vehicle may intentionally conceal mechanical issues in the car to induce the customer to buy it – a situation which will almost certainly be to the customer's detriment.

Going back to our hypothetical, what if an individual submitted to an organization an invoice which did not state any purpose? What if it included a price, contact info, etc. and simply requested money from the accounts payable folks? If nothing is offered in exchange, is it still fraud? I would argue that such an action does not strictly meet the definition of fraud. Allow me to explain.

People may assume, and we know how that goes, but this is an issue that can arise in court: someone may base an opinion on an assumption, and opposing counsel may object by stating that the speaker "assumes facts not in evidence". In our example, if the accounts payable team assumes that something of value was provided by the issuer of the invoice, but they do not check, they are making the same sort of assumption. If they pay the invoice without checking, has a fraud been committed?

We can go back to intent. One could argue that the sender of the invoice intended to induce Accounts Payable to send money; this is obvious as the existence and transmittal of the invoice are evidence of that. However, if the sender explicitly – openly and notoriously – excludes the purpose for the invoice on the invoice itself, how would one go about demonstrating intent? If pressed, the sender could say that he was simply asking for money with no offer – expressed or implied – to provide anything of value, and that could be true. However, if that is the case and the sender is relying on Accounts Payable to be sloppy and simply pay the invoice without looking too much into it, this would be more likely to fall into the category of "bad faith". Bad faith is defined (ibid) as simply "Dishonesty of belief, purpose, or motive".

From a hypothetical investigatory perspective, how could one go about determining whether the sender meant to transmit a simple request for money or if the sender genuinely acted in good faith but made a mistake? If we assume (there's that word again) that all documents and other items have been made available through discovery, we might look for other versions of the invoice: was there ever a version created that included the purpose of the requested payment? If the invoice happened to be for a dozen new mobile devices, did the sender have a completed order showing that the devices were in stock on their end? It is possible that the sender would need to order the devices once payment was made; in that case, does the seller have a documented business relationship with an organization that could provide the devices? If the seller purchased goods on a transactional basis from a retailer, there may not be a reseller agreement in place. Under those circumstances, we could look for additional communications from the purported customer. A purchase typically does not exist in a vacuum, so there should be a request of some kind originating from the customer organization asking for the invoicer to provide the mobile devices.

If there is no evidence of a correct invoice and no evidence of the seller's capability to provide the [allegedly] ordered devices to the customer, then we appear to be in bad faith territory. Is it fraud? That may depend on whom one asks. •

An Antitrust Case Against Google

Scott Zimmerman takes a look at another potentially significant legal action that's underway against the technology giant.

Editor's note: spending time on the internet, one may notice that some people have strong opinions about Google. It is also fair to mention that some internet users hold strong opinions about online ads. The case we are about to examine includes both Google and online adverts, but in the interest of unbiased exploration and discovery, we will not be discussing, for example, whether A is good or B is bad. We will instead be looking at the information that has been presented to the court, at the statute(s) under which the case was brought, and possibly offer some tentative interpretations regarding whether there appears to be a reasonable basis for the Plaintiff's complaints. So, we will look at the facts.

And Then Move On To Antitrust

In another instance of legal terminology diverging from more traditional English, "antitrust" is its own entity and despite the name is not the opposite of "trust". "Trust" in the legal sense generally refers to a relationship in which some resource(s) are owned by entity Y but entity Z is allowed to make use of the resource(s) for their own benefit. Essentially A is trusting B to keep an eye on things and to use the resource(s) in a reasonable fashion.

Antitrust, on the other hand, is a business-focused area and it concerns the conduct of organizations in addition to the conduct of individuals. One will frequently read in such cases statements like "CompanyCo is accused of…"; the conduct under discussion is often viewed as institutional and systemic rather than localised and specific. To define antitrust properly, we will consult the 10th Deluxe Edition of Black's Law Dictionary:

Antitrust law, n. (1890) 1. The body of law designed to protect trade and commerce from restraints, monopolies, price-fixing, and price discrimination. The principal federal antitrust laws are the Sherman Act (15 USCA §§ 1-7) and the Clayton Act (15 USCA §§ 12-27).

(The 'antitrust' entry is simply a redirect or pointer to the definition of 'antitrust law'.)

"Restraints" is fairly self-explanatory, but it would be useful to clarify the definition of "monopolies":

Monopoly, n. (16c) 1. Control or advantage obtained by one supplier or producer over the commercial market within a given region. 2. The market condition existing when only one economic entity produces a particular product or provides a particular service. ï The term is now commonly applied also to situations that approach but do not strictly meet this definition.

In brief, a monopoly is the practical suppression of effective business competition which thereby creates a power to control prices to the public harm. 54A Am. Jur. 2d Monopolies, Restraints of Trade, and Unfair Trade Practices § 781, at 107 (1996).

We will be primarily concerned with the first definition. In commercial environments this phenomenon may be described colloquially as "the 800lb gorilla", meaning that the largest entity is also the fiercest and thus capable of intimidating the lesser competitors.

The 1996 citation above brings up an interestingly specific word: power. The phrase "monopoly power" was captured in 1954 and points to what is likely the most substantial negative effect of a monopoly.

Monopoly power, n. (1954) The power to control prices or to exclude competition. The size of the market share is a primary determinant of whether monopoly power exists.

That citation specifies another key criterion for identifying monopoly power: public harm. It is possible for a single entity to be the sole provider of a good or a service, and to keep prices approximately where they would be if there were competition, but it is the harm to the public which draws attention to potentially monopolistic practices. If a single entity uses its might to quash competition, potentially via acts that are legal when considered individually, and to charge their customers – who have no alternative – essentially whatever they like, that is the source of the harm. It is relevant to note that in the 155-page DoJ complaint document, the phrase "monopoly power" occurs twenty-one times; from that we can begin to understand the plaintiff's view of the case.

Side note: we should clarify that there are some exceptions to this sort of monopoly: utilities such as water, electricity, and natural gas are frequently run by single entities because having multiple organizations running their own supply lines would be impractical at best (and potentially dangerous at worst). In such cases the single entity will be permitted to operate a monopoly, but the government will provide oversight and regulation – essentially taking the place of market-based competition and influence.

Department of Justice vs A Tech Company

Readers who were in (or were aware of) the technology industry in the late 1990s may recognize the description of the antitrust case in the opening paragraph: it is similar to the one brought by the DoJ against Microsoft in 1998. That case was largely based on complaints that Microsoft was intentionally a) trying to exclude other web browsers from personal computers in favour of its own Internet Explorer, and b) attempting to make Internet Explorer an integral and non-removable component of their Windows operating systems. The US government brought the case under the Sherman Antitrust Act of 1890 (the Sherman Act). That is not a typo: the Act was passed in the year eighteen-ninety. Because of the time period in which it was written, the language is extremely broad and surprisingly brief compared to modern legislation. We will largely be concerned with Sections 1 and 2 of the Act.

Section 1 states *"Every contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations, is declared to be illegal. Every person who shall make any contract or engage in any combination or conspiracy hereby declared to be illegal shall be deemed guilty of a felony, and, on conviction thereof, shall be punished by fine not exceeding $100,000,000 if a corporation, or, if any other person, $1,000,000, or by imprisonment not exceeding 10 years, or by both said punishments, in the discretion of the court." The dollar figures have been updated over the years; the original fine was $5000US.* ▷

Google is thought to have embarked on a campaign specifically to solidify their own position in the ad market by acquiring DoubleClick, an ad exchange called AdX, and an ad server called DFP.

Section 2 states *"Every person who shall monopolize, or attempt to monopolize, or combine or conspire with any other person or persons, to monopolize any part of the trade or commerce among the several States, or with foreign nations, shall be deemed guilty of a felony, and, on conviction thereof, shall be punished by fine not exceeding $100,000,000 if a corporation, or, if any other person, $1,000,000, or by imprisonment not exceeding 10 years, or by both said punishments, in the discretion of the court."*

What we can draw from this is straightforward: trade should not be restrained by any entity participating in the market. This applies equally to individual actors and to groups, operating both domestically and internationally. We can break it down a bit further: do not monopolize anywhere and do not conspire to monopolize anywhere, or there will be penalties.

What Did Google Do (Allegedly)?

The DoJ trial started in September and is expected to run well into November, so we will not have solid conclusions when this issue of DFM goes to press. Until a judgment is rendered, we will continue to describe the Defendant's actions as 'alleged'. In the meantime, we have a summary of the planned action from the complaint filed by the DoJ. In all there are five specific line items that capture the central themes of the case. Each Claim for Relief includes as an incorporated reference the first 309 paragraphs of the civil suit; the 3XX numbers below are the paragraph identifiers in the document.

First Claim for Relief: Monopolization of the Publisher Ad Server Market in Violation of Sherman Act § 2

312. Google has unlawfully monopolized the publisher ad server market through a course of exclusionary conduct described herein. While each of Google's actions increased, maintained, or protected its publisher ad server monopoly and/or market power in adjacent markets, the following exclusionary conduct–taken together–played a particularly important role in unlawfully establishing or maintaining a publisher ad server monopoly.

Remember the item above that mentioned how individual acts may be legal but taken in aggregate may become a problem? Google is thought to have embarked on a campaign

Several documents that had been entered into evidence were publicly exposed for an unknown period of time.

specifically to solidify their own position in the ad market by acquiring DoubleClick (the leading ad purveyor), an ad exchange called AdX, and an ad server called DFP. Taken individually, these actions would be considered normal business practises. However, when they are combined, and when Google allegedly excluded and otherwise limited competing ad-oriented entities' use of those facilities, they created the situation which led to the DoJ complaint. Specifically, Google is further alleged to have required their Ads customers to use AdX exclusively while allowing only DFP to have near-real-time access to AdX. One might see how these actions would be considered anticompetitive, and the DoJ complaint ties all of that together like so:

320. Although each of these acts is anticompetitive in its own right, these interrelated and interdependent actions have had a cumulative and synergistic effect that has harmed competition and the competitive process.

Because the remaining Claims for Relief include the first 309 paragraphs by incorporation, and because the summary justifications for Claims 2 and 3 are similar to the first, we will look at specific items that make each Claim different. For example, the next two items on the list form an interesting pair.

Second Claim for Relief: Monopolization of the Ad Exchange Market in Violation of Sherman Act § 2

Second Claim for Relief, in the Alternative: Attempted Monopolization of the Ad Exchange Market in Violation of Sherman Act § 2

This appears to be the DoJ hedging their bets. There seems to be enough evidence for a reasonable person to conclude that Google may be in violation of one or more pieces of the Sherman Act. The wording of the Second Claims indicates that there is interest in determining whether Google attempted to monopolise a market, or whether they tried to monopolise a market and were successful. Recall that this is a civil - rather than criminal trial - so the restriction on being tried twice for the same alleged actions does not come into play.

Third Claim for Relief: Monopolization of the Advertiser Ad Network Market in Violation of Sherman Act § 2

335. Google's exclusionary conduct lacks a procompetitive justification that offsets the harm caused by Google's anticompetitive and unlawful conduct.

Earlier in this article we touched on the idea of good business practises vs antitrust practises. Businesses are expected to compete in their

respective marketplaces and their goal is to make money, so one should not expect overly cordial relationships. The DoJ holds the opinion that what Google is alleged to have done goes beyond competition and has moved into antitrust territory.

Fourth Claim for Relief: Unlawful Tying in Violation of Sherman Acts § 1 and 2

337. Google's AdX and DFP are separate and distinct products. They are sold in different markets; their functions are different; there is separate demand for them; and they have been treated by Google and by other industry participants as separate products.

§ 1 of the Sherman Act has entered the chat. We are principally concerned in this Claim for Relief with the idea of tying – or bundling or packaging together – of disparate items in order to exert control over the unique combination that results. We saw earlier that Google is alleged to have created a one-to-one relationship between the ad exchange AdX and the ad server DFP. This was apparently done to leverage monopoly power and to create a critical marketplace conduit that would be solely under the control of Google, effectively excluding competitors.

Fifth Claim for Relief: Damages Incurred by the United States by Reason of Google's Violations of the Antitrust Laws, 15 U.S.C. § 15a

341. Google's violations of the Sherman Act have caused the United States to incur monetary damages, as the United States and its various agencies and departments are buyers of open web display advertising

Our last item is something of a curve ball as it is not strictly tied to antitrust law. In this case we are looking at the financial damage done to the US government. By using (and potentially abusing) its monopoly power, as believed by the DoJ, the other pieces of the US government that purchased advertising from Google paid higher prices than they would have done had the ad company not acted in the alleged monopolistic fashion. Extracting excessive revenue from the government may well be seen as a form of "public harm".

The Story So Far

When a trial is underway in the US court system, often there is an option for the general populace to observe: there may be a visitors' gallery for people to attend in person, for example, or there may be a webcast, etc. Near the beginning of this trial, Google successfully lobbied to make the proceedings private due to their concerns over potential disclosure of pricing and other trade secrets, so coverage is rather limited. However, there was some inadvertent sharing of information.

As typically happens in a proceeding, there is a phase of discovery. Essentially this allows the plaintiff's counsel to request specific information from the defendant which may be used to demonstrate the plaintiff's case. Common items to be requested are inter alia email messages, contracts, and internal training/briefing materials, as these items tend to contain valuable dates, figures, and other concrete details.

Much to Google's annoyance, several documents that had been entered into evidence were publicly exposed for an unknown period of time. Some interested observers of the proceedings downloaded copies of those documents and continued to make them publicly available. That list included several emails among Google marketing staff, but those are not the most interesting items. That title belongs to several slide presentations: Antitrust Basics for Search Team (March 2011); On Strategic Value of Browser Home Page to Google (April 2nd, 2007); On Strategic Value of Default Home Page to Google (March 27th, 2007); Search Entry Points on Android (September 28th, 2016); and Search Ads 101 (April 17th, 2020). Given the amount of secrecy that is in place at Google's request, it is not clear how much more information will be made available to the public.

Conclusion

As mentioned, the trial is expected to continue through the middle of November 2023. It is a civil trial and arguments are being heard by a jury, though of course there is a judge overseeing the proceedings. The DoJ has asked for some specific actions to be taken should the jury decide in their favour. In addition to clear and formal statements of agreement with the Claims for Relief, the DoJ has asked that Google be instructed to disconnect the Google Ad Manager suite from AdX and to disconnect AdX from DFP "… along with any additional structural relief as needed to cure any anticompetitive harm". This collection of changes to their core business practices would very likely be more disruptive to Google than the fines and court costs would be. We will know more next month – please stay tuned. •

REFERENCES

https://www.justice.gov/d9/press-releases/attachments/2023/01/24/us_v_google_complaint_0.pdf
https://www.theverge.com/2023/9/21/23883680/us-google-antitrust-trial-amit-mehta-doj-exhibit-documents
https://www.reuters.com/technology/verizon-executive-testifies-google-search-always-pre-installed-mobile-phones-2023-09-18/
https://apnews.com/article/google-antitrust-trial-search-engine-justice-department-2cfb06271455c7e12c4927959061e832
https://www.archives.gov/milestone-documents/sherman-anti-trust-act
https://www.law.cornell.edu/uscode/text/15/1

***Scott Zimmerman**, CISSP has been an Information Security practitioner, consultant, presenter, and trusted advisor for twenty years. He has been researching legal issues in computer forensics part-time for over ten years, and is working to bridge the gap between law and technology in this area.*

LEGAL News

23 And More People Than Intended

23andMe is a purveyor of genealogy services: customers use their provided kits to collect a saliva sample which is then sent to the company's laboratory. The lab folks work their magic to parse the DNA and provide a report, giving the customer details of the genetic makeup and ancestry they were able to identify. However, from the beginning there have been security concerns: users who purchase a service will of course need to provide their personal and payment information, but there genuinely may be sensitive information in the reports that the service generates. In addition to the potentially awkward misidentification of a father, there may be indicators that a specific individual is prone to certain conditions or diseases or may have outright lied about their own lineage for personal gain. (For example, there is at least one political figure in the US who has inaccurately claimed to have some percentage of ancestry in a particular group.) One might think, then, that the company would be paying extremely close attention to the security measures surrounding this sensitive data.

In early October, 23andMe announced that they had been the target of a credential-stuffing attack and that several customer accounts had been compromised. The attack works like this: one site is compromised initially, and the username and password pairs are stolen; these pairs are typically made available as a data blob on the dark web and elsewhere; and then those same pairs are directed firehose-style against another site. The attackers are banking on the assumption that people will reuse username/password pairs – despite all available guidance telling them not to do that. If PersonX uses myemailaddress/k1ttyk@t to log into site A, there is a non-zero chance that PersonX will use the same credentials to log into site B.

And that is what happened to 23andMe: the attackers simply blasted previously-known-good credentials at their site and they (the attackers) were successful, gaining access to a fair number of customer accounts. A recent blog entry from 23andme.com includes the following: "Since 2019 we've offered and encouraged users to use multi-factor authentication (MFA), which provides an extra layer of security and can prevent bad actors from accessing an account through recycled passwords." That sounds like a good idea, though perhaps it should be required rather than encouraged.

The FTX Story Continues...

In a previous issue we examined the alleged goings-on at FTX Trading Ltd., with Samuel Bankman-Fried (SBF) at the centre of the fray. As more of the story unfolds there are reports that other individuals, in addition to the original group of five (SBF, Daniel Friedberg, Zixiao "Gary" Wang, Nishad Singh, and Caroline Ellison), may have played significant parts in the alleged illegal activities.

From the beginning of his own legal journey, SBF claimed that his parents – Allen J. Bankman and Barbara Fried – were not directly involved with the suspicious flow of money into and out of FTX. However, it now appears those statements were not entirely accurate. According to a complaint filed in late September in the US Bankruptcy Court for the District of Delaware, Bankman and Fried were given and/or helped themselves to "millions of dollars" in gifts and cash. Also under dispute is their ownership of a villa in the Bahamas, which is reportedly worth over $16US million and which served as the erstwhile headquarters for FTX in the runup to the company's bankruptcy proceedings.

Somewhat surprisingly, the civil suit was brought against Bankman and Fried by (inter alia) the remaining members of FTX Trading LLC and Alameda Research, and the goals of the action are as follows: "Plaintiffs bring this action against Bankman for intentional and constructive fraudulent transfer, breaches of fiduciary duties, aiding and abetting breaches of fiduciary duty, unjust enrichment, knowing assistance or knowing receipt, and disallowance of claims; against Fried for [the same list]; and against both Defendants for damages, as well as to avoid and recover from Defendants (or from any other person or entity for whose benefit the transfers were made or obligations incurred) all transfers of property of Plaintiffs and all obligations of Plaintiffs to Defendants made prior to the commencement of the Chapter 11 Cases by Plaintiffs." That is an impressive list of alleged offences, but they may reasonably be summarized as "The Defendants paid themselves, their organizations, their causes, and their friends handsomely using money taken from FTX and Alameda, et al, and we would like it back now"; the inclusion of the intent to recoup funds from any of Bankman's and/or Fried's recipients is quite interesting. It's also worth noting that the civil suit itself actually uses the terms "piggy bank" and "lined their own ... pockets", so we have an understanding of the plaintiffs' viewpoint. •

We support British ex-military into cybersecurity & tech careers

RFEA | THE FORCES EMPLOYMENT CHARITY

TECHVETS

Building on the strengths of veterans

BECOME A MEMBER

- Join a leading ex-forces online community
- Train on cutting-edge cyber security platforms
- Access essential employment support

Are you an employer seeking to recruit top ex-military cyber security talent?

Join us:

email: team@techvets.co

Making Maximum Exploitation of Electronic Evidence More Accessible

Arsenal Image Mounter

Mount the contents of disk images as "real" disks on Windows® with powerful and unique digital forensics functionality

Hibernation Recon

Reconstruct active memory and extract multiple types (and levels) of slack from Windows hibernation files

Registry Recon

Unlock the potential of huge volumes of Windows Registry data and see how Registries changed over time

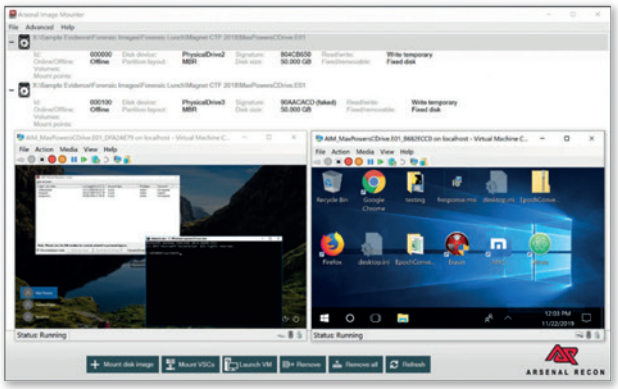
"After many unsuccessful attempts to launch forensic images into virtual machines with a popular digital forensics tool, I decided to give Arsenal Image Mounter a try. I'm very glad I did, because I was able to virtualize forensic images from multiple suspects. AIM also bypassed Microsoft cloud account passwords within the virtual machines, so I was able to take valuable screenshots for the US Attorney. In addition, I have found AIM's multiple methods of Volume Shadow Copy exporting to be useful."

-- ICE/Homeland Security Investigation

"Hibernation Recon has become DoD's must-have tool for extracting digital artifacts from Windows hibernation files. Not only does Hibernation Recon properly reconstruct active memory for all versions of Windows when other tools fail, it is the only tool that extracts various types of "slack space", which has yielded critical forensic artifacts for DoD's foreign intelligence mission that could not have been obtained any other way."

-- United States Department of Defense

ArsenalRecon.com sales@ArsenalRecon.com @ArsenalRecon

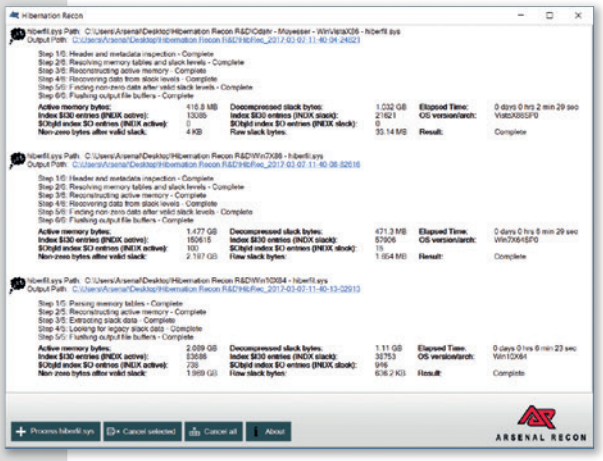


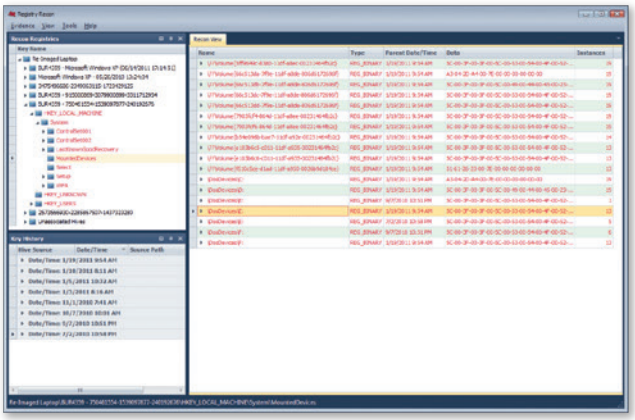
Arsenal Image Mounter

Arsenal Image Mounter mounts the contents of disk images as complete disks in Windows®. As far as Windows is concerned, the contents of disk images mounted by Arsenal Image Mounter are real SCSI disks, allowing users to benefit from disk-specific features like integration with Disk Manager, launching virtual machines (and then bypassing Windows authentication and DPAPI), managing BitLocker-protected volumes, mounting Volume Shadow Copies, and more.

Hibernation Recon

Hibernation Recon not only supports active memory reconstruction from Windows XP, Vista, 7, 8/8.1, 10, and 11 hibernation files, but also extracts massive volumes of information from the multiple types (and levels) of slack space that may exist within them. Additional features of Hibernation Recon include the automatic recovery of valuable NTFS metadata and parallel processing of multiple hibernation files.





Registry Recon

Registry Recon is not just another Registry parser. We developed powerful new methods to parse Registry data so that Registries which have existed on a Windows system over time can be rebuilt, providing unique insight into how Registry data has changed over time. Registry Recon provides access to an enormous volume of Registry data which has been effectively deleted, whether that deletion occurred due to benign system activity, malfeasance by a user, or even re-imaging by IT personnel.

Arm Yourself

Get the entire collection of Arsenal tools with an affordable subscription which:

- Enables the full functionality of all our tools with a single license
- Locks in a low price with discounts based on subscription length
- Provides easy access to new versions and support (no more SMS hassle)

Select the plan that's right for you at ArsenalRecon.com!

Controlling Digital Forensic Environments

Matt Carver-Smith analyses the benefits, techniques and equipment that promote secure, efficient computing environments.

The Forensics Science Regulator's Codes of Practice, prepared under Section 2 of the Forensic Science Regulator Act 2021, completed its approval by the Secretary of State and Parliament and came into force on 2nd October 2023.

These statutory requirements for forensic laboratories ensure sufficient controls are in place throughout Forensic Science Activities (FSAs) to meet the requirements of the UK judicial system. The new 'Codes' cover a range of areas relating to forensic activity. Most of these requirements are designed to enable traceability of actions, standardisation of approach, validation, and quality control of methods. However, meeting all these requirements in a busy digital forensic laboratory can prove difficult. This article is intended to help!

At CACI DFL, we utilise several domain and network-based technologies and techniques to make managing the forensic platform more efficient and streamlined. Here, I'd like to give an overview of some of these technologies.

We will dissect other techniques and equipment that can help deliver a consistent computing environment while still increasing efficiencies.

In a Windows domain environment, there are several available tools that form the fundamental building blocks of your computer network:

- Active Directory
- Group Policy
- Windows Server Update Services and Windows Deployment Services
- Centralised storage.

Throughout this article, we will review each in turn, exploring how you can benefit from the functionality available. Then, we will dissect other techniques and equipment that can help deliver a consistent computing environment while still increasing efficiencies.

Active Directory

Think of Active Directory, often referred to as simply AD, as the filing cabinet and index system of your network.

AD stores information about all the objects on your network in a logical, hierarchical structure. This is then presented to users and administrators in an easy form to manage.

AD works in close collaboration with Group Policy (which we will come on to). The structures defined within AD will determine what you can apply Group Policies to. For example, you may have a subgroup of users within the main user group that require additional and specific controls to be applied. The logical structure and members of that group would be created and managed in AD, but the Group Policy can be applied to one or each of the levels of the group differently. ▷

Simplifying The Deployment of a New 'Build'

Deploying your build using Windows Deployment Services simplifies and standardises the process. A workstation build is another opportunity for controls to be put in place. By managing local settings carefully, you can ensure that applications are installed in the same place, making later configuration much easier. Then, using WDS, you can make that build available across your entire network for others to rebuild from. By applying advanced configuration, you can even get that build to be automatically joined to your domain. The end user needs to do very little, but once complete, they have a fully built and approved workstation ready for use, with no need to reinstall Windows or an endless list of applications. This can save a lot of time when rebuilding workstations as end users can do most of the work themselves.

Benefits of Centralised Storage

We can leveraging centralised storage configuration options to maximise network storage. Typically, any network storage provides greater performance than traditional hard drives, as they will usually be configured to operate in a RAID (Risks, Assumptions, Issues, Dependencies), enabling the reading and writing of data across multiple disks.

Greater resilience can be achieved with a RAID depending on the specific configuration used. For example, a RAID 6 configuration can have up to two disks in the array fail without losing data integrity while still supplying faster read and write speeds than a single disk.

Data security can be more easily managed using Share and NTFS permissions when storing data on network storage. This can be as granular as needed, even limiting all file access to only those examiners and investigators required. Configuration files distributed through GPOs could be placed into folders where standard users are not authorised to make changes, preventing unmanaged changes.

Another benefit of using network or centralised storage is the reduction in preparation time required on a case-by-case basis. When using a hard drive in a workstation, there is a certain amount of work required to encrypt the disk and create a folder structure. Similarly, once a case is completed, there is no requirement to wipe that disk for subsequent reuse, saving more time..

This is great way to separate accounts with administrative rights from standard users. In fact, it's best practice for any user who requires an account with administrative rights and will also be a standard user to have two accounts separated in this way.

Another way of grouping users within AD is security groups. These security groups can be made of any number of users without impacting the grouping and any hierarchical structure already existing in AD. The groups can then be used to control access to network resources; for example, a real-world example of this might be that you wish to give access to some sort of resource to only those who are in the auditor's group. Using security groups, you could easily group these users together, regardless of where they may sit in the logical structure of the unit.

This example also demonstrates another added benefit of managing users in this way, if someone is no longer an auditor, they just need to be removed from the auditor's security group and they will lose any privileged access that they had, eliminating the need to manage each shared resource individually to remove access.

Furthermore, you can nest these security groups to ensure that being a member of one automatically makes you a member of another.

Ultimately, managing users and computers in this way saves time, as once the users and computers are in AD, any user can log on to any computer using their account due to the centralised nature of AD. It also ensures that users experience the required controls regardless of what computer they use as a result of its centralised management.

Group Policy

Group Policy is like a rule book for your network. It allows you to control configurations for users and computers using Group Policy settings and Group Policy Preferences. A group of these settings is known as a Group Policy Object, sometimes referred to as a GPO.

In a Windows domain group, policy settings and preferences can be centrally controlled through the Group Policy Management Console. As mentioned earlier, by carefully structuring AD and applying GPOs, security, management, and functionality can be standardised across the entire network.

GPOs can be applied at the root of your AD hierarchy to enforce these settings across all workstations, for example. This is an ideal way of enforcing Windows password complexity, age, and history requirements. GPOs can help save you time with workstation encryption by configuring your BitLocker requirements once and applying it to the required group of workstations. Managing BitLocker in this way, recovery keys can also be kept in AD, ensuring you don't lose them.

Once you start using GPOs, you will find that they are incredibly powerful and can be used to control or manage almost all elements on your domain, including Windows desktop, screen lock out settings, lock screen, drive mapping, time zone controls and much more.

In a digital forensics' lab, you might also want to be able to apply more fine controls around applications. Perhaps you've decided on the settings used for processing in a particular tool and you want to ensure everyone is using the same settings. Using a GPO, you can verify that the same configuration or settings are being enforced on a group of users or workstations in AD. This enforces consistency, as the settings are continuously being controlled but also results in only a single change, and that change is made across all affected workstations almost instantaneously, without having to make changes in configuration on all of your workstations one at a time.

Where configuration might vary between certain versions of an application, there are techniques that can be used in Group Policy to ensure that the correct configuration is applied to a workstation based on that software version.

GPOs can also be used to help you improve your networks security and resilience. For example, Windows Defender can be configured to run at specified periods, helping to identify any issues that might arise. ▷

Policy	Security Setting
Enforce password history	24 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	12 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Not Defined

Figure 1. GPO Password Policy

Benefits of Virtual Workstations

By making greater use of a large concentration of computing power through virtualisation we are able to create:

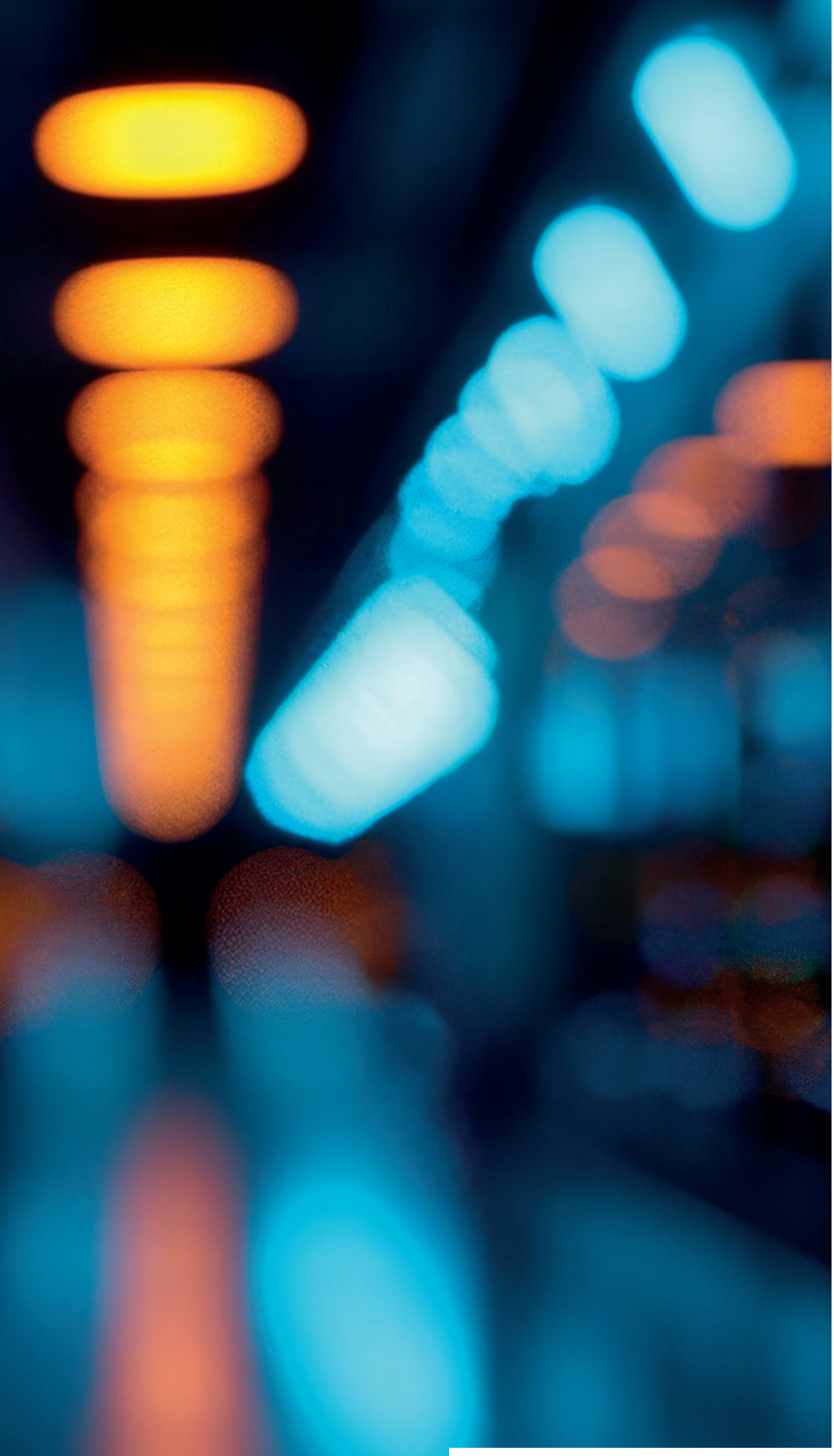
- *Environments capable of running ten or more workstations on one server by using a virtualisation platform like Microsoft's Hyper-V in conjunction with Remote Desktop Services. The configuration of a collection of virtual computers is based on a 'template' machine. This is then used to build as many workstations as required, or at least as many as your available resources allow.*
- *Identical workstations that are all clones of the original template.*
- *When a user has finished with their virtual workstation, it is rebuilt back to that original configuration.*
- *Each time a user logs on, they know the exact setup of the device and the applications installed on it.*
- *Examiners can have multiple workstations available to them, allowing processing to be done in parallel.*
- *Easy to adjust the resources available to each or adjust the total number of workstations available within the bounds of available resources.*

EXPERT TIP: Use Multiple Builds

You don't have to have only one build available. You may make different builds available depending on how you structure your workstations and how you logically operate. By keeping records of your builds, you could deploy an old build if, for example, you needed to perform some historical work. Availability of the builds is something manageable by your administrator and many builds can be kept, with only certain ones made available to further control the environment.

WARNING: Network storage might be the only solution

These are the basic concepts of network or centralised storage, but depending on the solution, storage capabilities and options can become far more complex yet still deliver greater performance, security, or resilience. Realistically, for some exceptionally large cases, this kind of storage solution can be the only practical solution dependant on how many interfaces you have for internal disks.



Leveraging useful information from BGInfo

By compiling device and application information into one place we are able to enhance visibility.

Workstation:	**DFL0014**
Boot Time:	27/11/2023 16:00
OS Version:	Windows 10
Build:	1.0
FTK Imager:	4.7.1.2
EnCase Imager:	7.10.0.103
Cellebrite UFED:	7.66.0.126
Cellebrite PA:	7.62.2.9
Axiom:	7.4.0.36841

Figure 2. BGInfo

BGInfo, is a Sysinternals program, can display all kinds of information about a Windows machine overlayed on the desktop background. In fact, you can use it to manage the desktop background and to create your own variables using the 'Custom' option. These can display environment variables, contents of a file, a registry value or a file's version information. This enables the creation of custom variables for any applications you want to track the version of and display them with any other useful information on-screen. If you're using some sort of build management, the file contents can read a text file that stores the build number or reference, for example, by placing BGInfo in the Windows startup folder, this information will be displayed and updated each time the machine boots. The settings you select are recorded in a .bgi file. Utilising some of the other techniques we've discussed in this article, this file could be centrally stored to prevent unauthorised changes and distributed using GPO to ensure all workstations have the latest version. BGInfo can be re-run either on demand by creating a custom shortcut or on a routine basis by using Windows Scheduler to ensure the information displayed remains up to date.

Once you start using GPOs, you will find that they are incredibly powerful and can be used to control or manage almost all elements on your domain, including Windows desktop, screen lock out settings, lock screen, drive mapping, time zone controls and much more.

Windows Server Update Services and Windows Deployment Services

DF networks are typically 'dark sites', a term referring to the network effectively being cut-off from the internet. Sometimes this is absolutely the case; other times, this is done using logical segregation within firewalls and switches.

Where segregated logically in this way with strict firewall rules, internet access can provide access to Windows updates via Windows Server Update Services. This is a service that is typically ran on a server to collect Windows updates based on a set of defined options. These updates can then be made available to other computers on the network, again with the help of a GPO. This time, the GPO will tell the computer where to look for updates, but can also control when the check is done, whether updates are automatically applied, whether the update process can be stopped by the user, etc.

At CACI DFL, we enforce regular checks for updates, but don't enforce the installation. Instead, we enable examiners to determine the best time to prevent a reboot being required in the middle of processing case work.

Once you've got your workstations all set up. you're managing your users in AD and your configuration with GPO; what happens if you must replace some computers, or your team expands, and you need to get those workstations up and running quickly? Using Microsoft's Deployment Toolkit (MDT) in combination with Windows Deployment Services (WDS), you can capture one of your workstations and make that deployable over your network as a network bootable option.

Centralised Storage

Implementing some sort of centralised storage enables many benefits: a reduction in data movement, improved performance, greater resilience, and an increased ability for the data to be secured and/or segregated. This could be an enterprise type SAN providing petabytes of storage or some sort of NAS.

A reduction in data movement reduces the need for continuous verification that data has been copied accurately, as it can be acquired to the central storage and processed there.

Other Techniques

So far, we've explored some of the functions available in a Windows domain, but there are other things that can be done to further augment your domain and the resources you have at hand.

- **Virtualisation** – Virtualisation is the concept of running a computer within another computer. There can be all sorts of reasons for doing this, like sandboxing to investigate malware, or to emulate another computer during an investigation.

- **Licensing** – Most forensic applications utilise some sort of dongle to license the product for use. Typically, you need that dongle to be plugged into the machine you want to run the application on. Keeping track of these dongles can often be troublesome. When examiners go on leave and lock workstations, dongles get locked in drawers or just plain lost. Using these dongles can be particularly tricky if using any virtualisation as there is no way to plug the dongle in!

- **Configuration Management** – Even if you are using some sort of build management, it is not easy to know immediately what applications are installed on a workstation at any one time. You could open each application and check the version. Or you can look in Control Panel at the 'Uninstall or change a program' list, but that's a bit clunky and some applications don't install in the traditional sense so don't get listed in there (think X-Ways, DCode etc.). Perhaps you manage your applications based on a build – but how do your users know what build they're using? Perhaps you want to know the IP address of the computer or the machine name?

By combining the technologies and techniques outlined above, efficiency savings can be realised that also have the knock-on effect of helping to control your forensic environment. By using tools like AD and GPO, the digital forensic environment can be made easier to manage and maintain. •

By combining the technologies and techniques outlined, efficiency savings can be realised that also have the knock-on effect of helping to control your forensic environment.

Q&A

While some licenses can be converted to network or software licenses, replacing the dongle isn't always the most practical method, as you are then limited to only using your application on the network, what if you still want to take that license to a scene?
There is a hardware device called a dongle server which has many USB connectors where dongles can be plugged in. These dongles can then be connected using a client application on any workstation, virtual or physical, on the same network. If a dongle is in use, other users can see that it is in use and by whom. The device can be managed via a webpage hosted on the device itself, where administrator users can manually disconnect users from dongles if required.

Matt Carver-Smith *is a Digital Forensic Analyst for CACI Ltd. with over 11 years experience in digital forensics. Before working for CACI, hw spent 17 years at Humberside Police, the last 10 of which were in the Digital Forensics Unit. He started out as a digital forensic analyst specialising in computers, but as technology evolved and the demands on his unit grew, it became necessary to adopt new technologies like virtualisation, and he realised that the benefits were huge. He now has over 7 years experience implementing and managing digital forensics infrastructure, including servers, SAN storage and virtualisation. Having worn other hats throughout his career, like being an auditor or assisting with the technical aspects of accreditation, he could also see that these technologies could help to achieve their goals.*

CYBERSEC INNOVATION PARTNERS

INTERNET SECURITY VALIDATION AND ASSURANCE

WHITETHORN®

WHITETHORN® SHIELD

CONTACT US: INFO@CYBERSECIP.COM

Professionalising The Security Testing Industry

Emily Kinsella tames the Wild West of Security Testing.

There is currently an inherent lack of trust in the cyber industry between the buying community and the service industry. This is in part caused by the lack of understanding that surrounds cyber security specialisms'; whilst members of the general public understand the gist of what a cyber security professional or generalist does, the more niche specialisms can be a mystery. Most people know that a GP is a doctor. However, the same people may not know exactly what a chiropodist or a proctologist specialises in. In the same way many people will have somewhat of a grasp on what a generalist cyber security professional may do, but most likely won't know exactly what a security tester does.

There unfortunately is also an issue with some less than honest people in this industry selling services that are unnecessary. When members of the buying community have been burnt in this manner, they tend to develop a lack of trust for the industry in general, only aggravated by the mystery around the services offered as opposed to the services required for their bespoke needs.

By professionalising the industry and introducing clear career pathways the buying community will be presented with a list of trusted cyber security professionals, creating a more positive and trusting relationship between the buyers and the professionals offering the services. Clear career pathways will also greatly benefit both those seeking a career in the cyber industry and the employers with cyber roles they are seeking to fill. The recent IPSOS report: "Cyber Security Skills in the UK Labour Market 2023" found that there was a 33% increase in cyber security job postings from 2021 with over 160,000 relevant job postings in 2022. The demand is clearly there, yet there is the much-discussed cyber security skills gap preventing these roles being filled... or perhaps the issue is not a lack of skilled applicants; but unclear pathways to cyber careers and a lack of enthusiasm when it comes to upskilling current employees and entry level starters?

So How Do We Professionalise the Industry?

These issues can be addressed by introducing clearer pathways and structure to the profession. Up until now cyber security has been an unregulated industry with a lack of clarity for both those looking to join the industry and those looking to procure cyber security services. A recent example of a structured pathway is the introduction of the Cyber Advisor scheme. Before this was brought into place anyone could claim to be a Cyber Essentials expert, and there was no straightforward marker for those looking for a consultant to assist them. With the Cyber Advisor scheme there is now a clear, NCSC-certified marker of excellence; both the individual and the company they work for have to go through a rigorous process, with the consultant required to sit an exam, an interview, and further training before they can be accredited as a certified Cyber Advisor by IASME on behalf of the NCSC. ▷

How Chartership Differs from Check

The CHECK accreditation scheme differs from chartership in that the organisation is CHECK accredited as opposed to the individual. CHECK is the term used for the NCSC (National Cyber Security Centre) approved security testing organisations. CHECK is required for government departments and their associated agencies. CHECK is awarded to companies to illustrate they have the ability and methodology to provide CHECK level testing. Chartership is for the individual and does not rely on the individual's current employer. The chartership scheme will create a clear indicator of an individual's experience within the industry, as opposed to the clearance level/ability of the organisation they work for. Where the CTM and CTL level example are relevant for both schemes the end goal is different.

Currently there is an inherent lack of trust in the cyber industry between the buying community and the service industry. This is in part caused by the lack of understanding that surrounds cyber security specialisms.

EXPERT TIP

When applying to become charted or any level of membership ensure you thoroughly read the professional standard for security testing, this will massively help you with your application. When writing your application make sure to follow the STAR model: Situation, Task, Action, Results. This is also an excellent opportunity to detail the papers you have contributed to; this can include papers published in recognised journals, in-house publications, conference and seminar presentations, and any other contribution to industry, national and international bodies.

Standardising The Different Routes into Cyber

As we have mentioned, professionalising the industry has to involve addressing the cyber skills shortage as well as accrediting those professionals already working in this field, in order to meet the growing need for trusted cyber security professionals in the UK. There are plenty of cyber security degrees available for those looking to pursue a cyber career, including dedicated ethical hacking and security testing options. However, as many graduates have found these do not always lead to getting a job as a security tester. Part of this is again due to the lack of clear pathways within the industry. If there are hundreds of cyber degrees out there, how do you know which one will fit your needs and carry the most weight when it comes time to job search? The NCSC have a database of degree courses accredited by them which can help when making choices for academic study. Whilst a degree is by no means necessary to pursue a career in security testing this may be the path best suited to certain people. There are many accredited options out there, at both undergraduate and postgraduate level. Multiple universities throughout the country are included in this list, such as Abertay, Oxford Brookes, and Cardiff University.

Another route into a security testing career is to undertake a cyber security apprenticeship and then specialise in security testing. Apprenticeships are a valid option for people looking to take up a career in security testing that do not want to go to university. In contrast to many industries where apprenticeships can be dismissed by older professionals looking to switch careers, cyber security has a plethora of well-established apprenticeship schemes that provide a great route into the industry. Again, the NCSC database lists those apprenticeships endorsed by them.

Professional qualifications - CHECK

Currently in the United Kingdom the CHECK scheme is the symbol of excellence for security testers. CHECK is the term for the NCSC approved penetration test companies and the methodology used to conduct a penetration test. Companies providing CHECK services do so using staff who hold NCSC approved qualifications and have suitable experience. Penetration tests are conducted using NCSC recognised methods and the subsequent report and recommendations are produced to a recognised standard.

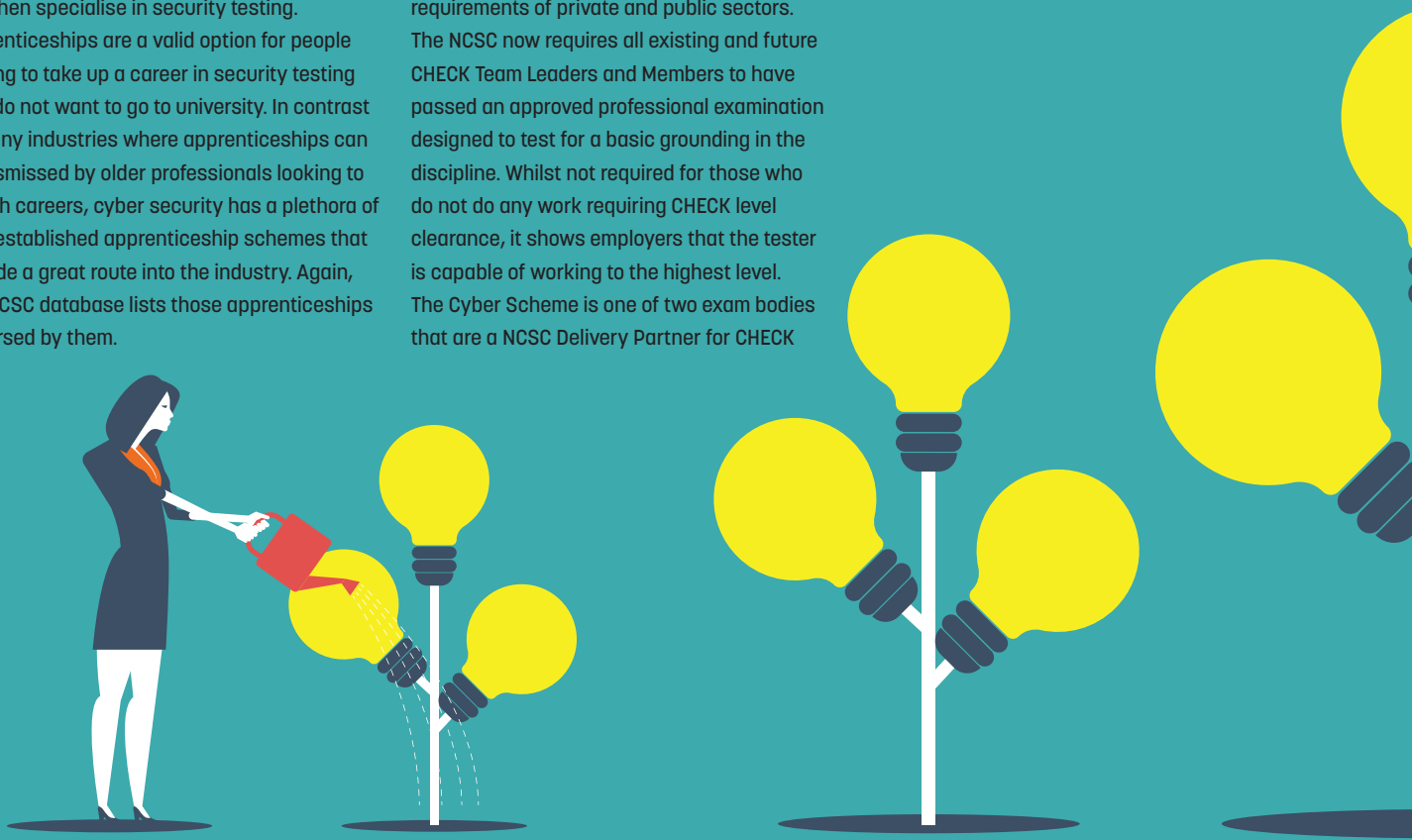
NCSC traditionally provided IT health check services to identify vulnerabilities in IT systems and networks which may compromise the confidentiality, integrity or availability of information held on that IT system for HM Government and the wider public sector. Due to growing demand, a partnership with industry was deemed necessary. The IT Health Check Service, or CHECK, was developed to enhance the availability and quality of the IT health check services that are provided to Government in line with HMG policy. Companies belonging to CHECK are measured against high standards set by the NCSC.

The NCSC and The Cyber Scheme work in collaboration to provide a set of examinations that are acceptable to industry and meet the requirements of private and public sectors. The NCSC now requires all existing and future CHECK Team Leaders and Members to have passed an approved professional examination designed to test for a basic grounding in the discipline. Whilst not required for those who do not do any work requiring CHECK level clearance, it shows employers that the tester is capable of working to the highest level. The Cyber Scheme is one of two exam bodies that are a NCSC Delivery Partner for CHECK

What Is Expected of a Chartered Security Tester?

A ChCSP must be able to demonstrate that they are working at the associate level by meeting the following criteria:

- *Be able to demonstrate their knowledge, understanding and experience relating to their specialism, including an understanding of cyber security in its widest sense and should be able to demonstrate knowledge across a number of security specialisms'.*
- *Be able to demonstrate that they have effective communications and interpersonal skills to operate at all levels within and without an organisation, with their peers and those who have little or no knowledge of cyber security.*
- *Be able to demonstrate that they have developed effective management skills and are able to demonstrate their ability to lead and mentor groups and individuals in a personal, technical, or business cyber security environment.*
- *Be able to demonstrate that they have the highest level of integrity, morals, and ethical values.*
- *Be able to demonstrate that they are committed to the continued development of themselves and the profession.*

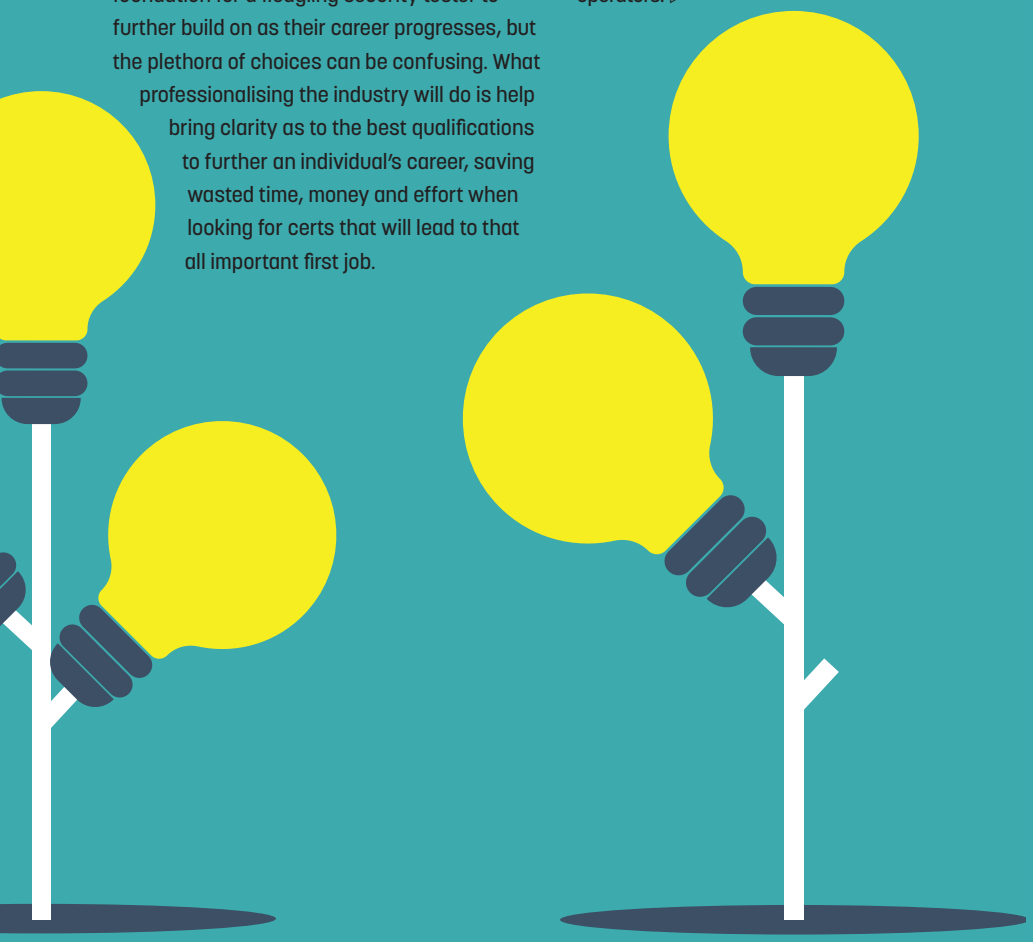


approved security tester exams. There are currently two levels of exam offered: team member and team leader. These exams are for those who are already working as a security tester, starting at practitioner level. The Cyber Scheme is also developing an entry level exam bridging the gap between leaving a cyber security-specific education and needing to work at practitioner level; this will coincide with the launch of the Chartership scheme as the exams will map to the different levels of chartership awarded to security testers. We believe this is a much-needed development in the standardisation of this industry; as a recognised assessor of excellence at the higher CHECK levels, The Cyber Scheme are well placed to meet the needs of industry and of individuals at this foundation level, aiding their career development through trusted and regulated pathways.

There are other professional qualifications currently available for entry level security testers provided by institutions including CompTIA, ISACA and (ISC)2. These entry level exams tend to be focused on cyber security as a whole, as opposed to specialising on security testing. They do create a good foundation for a fledgling security tester to further build on as their career progresses, but the plethora of choices can be confusing. What professionalising the industry will do is help bring clarity as to the best qualifications to further an individual's career, saving wasted time, money and effort when looking for certs that will lead to that all important first job.

Professional Training

There are many ways to progress a security testing career through further study, one of these methods being through professional training. The Cyber Scheme is one of the industry leaders in this field. Training is always face to face and is tailored to each individual cohort in order for practitioners to identify knowledge gaps and prepare for any future examinations. Our trainers discuss what areas the delegates need to concentrate on, focussing on what they actually need help with and not going over areas of established knowledge repeatedly. By utilising this method of creating a bespoke training programme for our participants we are able to give them a well-rounded education for security testing with real world applications. Unfortunately, training within the cyber security profession is still largely unregulated and the quality varies hugely; while companies like The Cyber Scheme aim to provide top tier training the responsibility still lies with the delegate to research different options and be sure their needs are being adequately met. There is hope that the professionalisation of the industry through Chartership will have a trickle-down effect on training and certification, creating trusted options with established and accredited operators. ▷



What is Expected of a Principal Security Tester?

A PCSP must be able to demonstrate that they are working at the principal level by meeting the following criteria:

- *Be able to demonstrate their knowledge, understanding and experience relating to their specialism, including experience of cyber security in another specialism.*
- *Be able to demonstrate that they have appropriate communication and interpersonal skills to fulfil their role with their organisation. This includes communicating with those who may have little or no knowledge of cyber security.*
- *Be able to demonstrate that they have developed management skills and are able to demonstrate their ability to lead groups and individuals in a personal, technical, or business cyber security environment.*
- *Be able to demonstrate that they have high levels of integrity, morals, and ethical values.*
- *Be able to demonstrate that they are committed to the continued development of themselves and the cyber security profession.*

What is Expected of an Associate Security Tester?

An ACSP must be able to demonstrate that they are working at the associate level by meeting the following criteria:

- *Be able to demonstrate their knowledge, understanding and experience relating to their role, some understanding of cyber security in its wider sense, and practical experience within their career.*
- *Be able to demonstrate that they have reasonable communication and interpersonal skills.*
- *Be able to demonstrate that they understand the need to develop management skills and have carried out some supervisory activity within a cyber security environment.*
- *Be able to demonstrate that they understand and apply integrity, morals, and ethical values.*
- *Be able to demonstrate that they carry out and plan for continued development of themselves and the profession.*

A cheap, but largely unregulated option for aspiring security testers is access to the free online game-based tools such as 'Hack the Box' or 'Try Hack Me'. While these tools are a good resource, it is important to bear in mind that they do not provide a complete security testing education, and do not provide sufficient information or support on the ethics and human aspects of hacking. These tools have exploded in popularity and there is a concern that the lack of clarity around the ethics of hacking is another issue created by a largely un-professionalised industry. It is hoped that in the future junior security testers will be able to demonstrate, by becoming Chartered at Associate level and thereby attesting that they only use their skills ethically, will help protect buyers from unscrupulous operators or, worse, threat actors pretending to be the good guys.

The UK Cyber Security Council (UKCSC)

Professionalisation and standardisation of this industry is being driven by the UK Cyber Security Council. The UK Cyber Security Council was introduced in March 2021 to be an independent body that sets standards and define career and learning paths for the cyber security industry. The UK Cyber Security Council provides a "single governing voice for the industry to establish the knowledge, skills and experience required for a range of cyber security jobs, bringing it in line with other professions such as law, medicine, and engineering."

The council was brought into place due to The National Cyber Security Strategy 2016-2021 policy paper that set out the UK Governments' plans to make Britain cyber secure and resilient in cyberspace. Included within this report was the government's desire to further develop the cyber security industry and accredit the profession by "reinforcing the recognised body of cyber security excellence within the industry and providing a focal point which can advise, shape and inform national policy."

The Department for Digital, Culture, Media, and Sport (DCMS) won the bid to commission the UK Cyber Security Council delivering it to a consortium of cyber security professional bodies known as the Cyber Security Alliance. The Institution of Engineering and Technology describe the Cyber Security Alliance as "a consortium of cyber security organisations that represent a substantial part of the cyber security community in the UK. It brings stakeholders together in the interest of advancing a healthy cybersecurity sector for the UK, from the development of professional recognition to the collaboration around acknowledged priorities to move the workforce and skills base forward."

The basis of the 2025 strategy for UK Cyber Security Council is set in five pillars:

- Professional Standards: Setting the standards for practitioners across the sector
- Professional Ethics: Creating and ensuring cyber professionals adhere to our Code of Ethics
- Careers and Learning: Providing guidance on how to join and progress within cyber security
- Outreach and Diversity: Striving for an inclusive and representative sector
- Thought Leadership and Influence: Positioning the Council as the voice of the profession

The chartership scheme is in its pilot stage, which is expected to run for most of 2023.

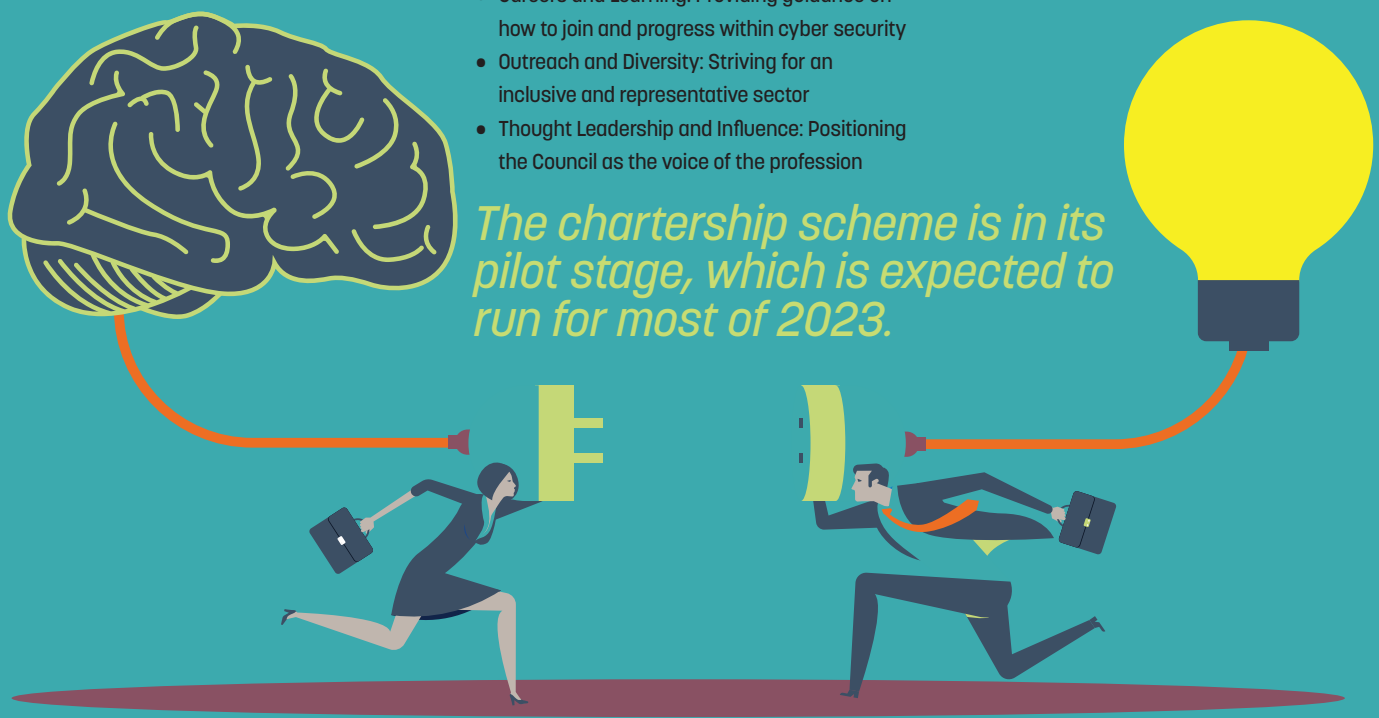
TOP FACT

The 2023 Ipsos report found that 53% of cyber sector businesses have tried to recruit someone in a cyber role since the beginning of 2021. The average number of job openings per company has risen from 5.2 in 2021 to 6.8 in 2022 and 8.2 so far in 2023. The jobs are out there, we just need adequately skilled and supported cyber security professionals to fill them.

Q&A

What will being chartered do for me?

Chartered status will enhance your CV and will help you find greater opportunity for career progression and with this comes an increase in earning potential. Gaining charted status demonstrates your commitment to professional standards such as the Council's code of conduct, practice, and ethics. This also proves an ongoing commitment to your continued professional development to ensure your expertise and competence evolves, is up to date and relevant. By aligning your experience and expertise with your area of specialism in cyber security to a nationally recognised standard of competence you clearly demonstrate your level of expertise. This further demonstrates that you belong to a network of respected and prestigious cyber security specialists.



Chartership

The UK Cyber Security Council is in the process of introducing a new Chartership scheme across the industry, with specific specialisms aimed at specific sectors within cyber security, as well as a generalist option. Cyber professionals will be assessed for the Professional Registration Titles of Chartered, Principal and Associate, providing assurance to all stakeholders and meeting the needs of a diverse range of organisations within the profession, without creating unnecessary barriers to entry, or progression for professionals. This is part of their commitment to helping make the UK become the safest place to live and work online. Additionally, this will also help to bring the cyber sector in line with other professions such as engineering or accountancy, which already have successful models for providing chartered professionals. The overarching aim is to bring clarity for both cyber practitioners and employers across the UK looking for cyber expertise by introducing a universally recognised professional standard for the industry.

The Security Testing specialism is currently in Pilot stage, and The Cyber Scheme are supporting the Council in the development and running of this pilot with the eventual outcome of becoming a Licensing Body for issuing charterships in Security Testing. Our hope is that this scheme will help bring clarity to the security testing industry, illustrating clear career pathways, and highlighting excellence within the industry.

What Does Chartership Mean for The Industry?

By establishing the chartership model within the security testing industry the council creates a clear pathway for aspiring and current security testers. For example, to be a fully-fledged chartered member they need to be well established in their career, having significant practical knowledge in several specialisms, and should have a particular specialism at which they are an acknowledged expert. A Chartered level security tester should be operating at a level where their professional opinion may reasonably be sought to contribute to the development of the overall cyber security profession. By creating a professional standard, the council will help to establish what skills and competencies should be associated with each level of security testing. This clear route map will help bring cyber security as a whole, including the security testing specialism, in line with other professions that already have a successful chartership model established.

Once a security tester has achieved chartered status, they will be required to continued professional development to maintain it. There are multiple different ways to earn continued profession development, or CPD, points; one of the simplest ways is by attending conferences and lectures. However, CPD points can also be earned through work-based learning, professional activity, formal education, and self-directed learning. CPD is a requirement to illustrate continued professional growth and that the individual is keeping up with new ideas and technologies. In an industry that evolves quickly, this is vital.

The chartership scheme is in its pilot stage, which is expected to run for most of 2023, and as such is constantly evolving and is subject to change. Each specialism will run its own pilot and the length will depend on the complexity and the number of stakeholders involved. What will not change is the stabilising influence regulation will bring to the industry, encouraging new talent to the industry with clear pathways and career progression.

Professional Standards Working Group

The UK Cyber Security Council has formed a Professional Standards Working Group to create and uphold the professional standards they are introducing; The Cyber Scheme's Strategy Director Andy Jones has been appointed as the Chair of the group. Andy has dedicated many years contributing to the development of the UK's cyber security industry, including a two-year period as service owner for several CESG (now NCSC) assured services covering product assurance, Certified Consultancy, Cyber Essentials, and Assured Penetration Testing (CHECK). The function of The Professional Standards Working Group is to contribute critical sector knowledge, enabling innovation and thought leadership. This will be achieved by widening community participation within the cyber security profession, shaping recommendations following pilot programmes, raising awareness of cyber security specialisms', collaborating with core council working groups, and defining professional titles. Commenting on his appointment, Andy said: "Cyber Security presents many challenges as society embraces the technology transformation that touches every aspect of life. As Chair of the PSWG I am pleased to be working with the UKCSC and colleagues from across the industry who bring a deep understanding of the challenges and the professional standards needed now and going forward." •

REFERENCES

Office, C. (2016). National Cyber Security Strategy 2016 to 2021. [online] GOV.UK. Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

UK Cyber Security Council. (n.d.). Ethics and the cyber security profession. [online] Available at: https://www.ukcybersecuritycouncil.org.uk/professional-standards/.

UK Cyber Security Council. (n.d.). Professional Titles. [online] Available at: https://www.ukcybersecuritycouncil.org.uk/professional-standards/chartership-and-professional-titles/#:~:text=Provide%20confidence%20and%20assurance%20of

UK Cyber Security Council. (n.d.). How to Become Chartered. [online] Available at: https://www.ukcybersecuritycouncil.org.uk/professional-standards/how-to-become-chartered

UK CYBER SECURITY COUNCIL STANDARD FOR PROFESSIONAL COMPETENCE & COMMITMENT (UK CSC SPCC). (n.d.). Available at: https://www.ukcybersecuritycouncil.org.uk/media/un0j1eur/v-4-21-12-22-uk-csc-spcc.pdf

Emily Kinsella *is the Marketing Executive for The Cyber Scheme. Emily has a BA in international Journalism and a master's degree in International Public Relations and Global Communications. She is involved with increasing the awareness and understanding of The Cyber Scheme, contributing to multiple articles on subjects including diversity in cyber, skills gap analysis and outreach to The Cyber Scheme's sponsor community.*

Nuclear Security LEADERSHIP

Richard Piggin highlights good practice for cyber security leadership.

The Office for Nuclear Regulation (ONR) undertook a series of board level briefings, in partnership with Accenture, across the UK civil nuclear sector in early 2023. The briefings covered the nuclear fuel cycle including fuel enrichment and manufacture, generation, and decommissioning. These briefings highlighted the importance of embedding an effective strategy, supported by strong leadership, governance, risk management and a positive security culture. [1] Paul Shanes CSyP FSyI FBCS, ONR's Head of Cyber Security Regulation, provided additional context to the author:

The briefings demonstrate ONR's enabling approach to regulation. They provided an opportunity to communicate recent updates to the UK national and civil nuclear cyber security strategies whilst leveraging Accenture's knowledge of relevant good practice from other critical national infrastructure sectors. This work supports our role as the UK's independent nuclear regulator and is key to delivering our mission to protect society by securing safe nuclear operations. [2]

This article highlights relevant good practice, relating it to the requirements of the civil nuclear sector and is based upon the materials produced to support executive briefings and has wide applicability to the leadership and governance of cyber security in other organisations.

ONR have since undertaken a series of inspections to assess the cyber security leadership and risk management arrangements. Initial findings suggest improvements are necessary from some dutyholder leadership teams; in defining their cyber security strategies and ensuring they have the skills to understand and manage specific cyber security risks. [3]

Protecting Nuclear Safety

In May 2022, the Department for Energy Security & Net Zero published the 2022 Civil Nuclear Cyber Security Strategy. [4] It builds upon the developments made in the sector since the initial strategy was published in 2017, which focused upon ensuring that the civil nuclear sector could defend against, recover from, and be resilient to evolving cyber threats (Figures 1 & 2).

This necessitates the protection of generating facilities, legacy facilities, new build projects and supply chains for civil nuclear from cyber-attacks that could compromise Sensitive Nuclear Information, disrupt electricity supply, damage facilities, delay hazard and risk reduction, and risk radiological consequences to workers, the public or the environment. The World Economic Forum Global Risks Report 2023 highlights the immediacy, as "widespread cybercrime and cyber insecurity" is a new top 10 ranked risk for the next decade, with more aggressive and sophisticated attacks targeting greater widespread exposure. [5]

The 2017 strategy defined roles and responsibilities, along with commitments and expectations for HM Government, UK Civil Nuclear Dutyholders (responsible persons on nuclear sites subject to security regulation), the civil nuclear supply chain, and Regulators, including the Office for Nuclear Regulation and the Information Commissioner's Office. The 2022 strategy continues the cross-sector partnership, being developed with UK civil nuclear organisations, the Office for Nuclear Regulation, and the National Cyber Security Centre. The strategy outlines how the sector will deliver four key objectives by 2026:

What is Operational Technology or OT?

According to the UK National Cyber Strategy (2022), "Operational Technologies (OT) – combine hardware and software to monitor, control and automate physical processes, particularly in industrial sectors such as energy, manufacturing, water, and transport." [24]

The networking convergence of IT and OT has bridged functionally distinct silos. Critical business systems run and administer the business and control systems automate real-time physical processes that enable the business to run. IT focuses on agility with frequent software patching, often with confidentiality foremost. Whilst OT environments demand high availability with integrity, in a reliable and stable environment, with safety paramount.

IT and OT technological convergence has also left systems exposed. OT systems are vulnerable to both old and new cyber threats, creating operational risks, with loss of availability increasing likely. The cyber physical nature of systems creates process safety hazards, increasing risks to safety, systems, and reputation.

Unsophisticated attackers may gain access to OT, and apply ransomware or interfere with systems, however, sophisticated actors behave like engineers, seeking to understand the process under control, developing attack strategies to create defined outcomes. Advanced attacks target the physics of the industrial process, such as flow, motion, temperature, level, flow, pressure, time/rate and process analytics.

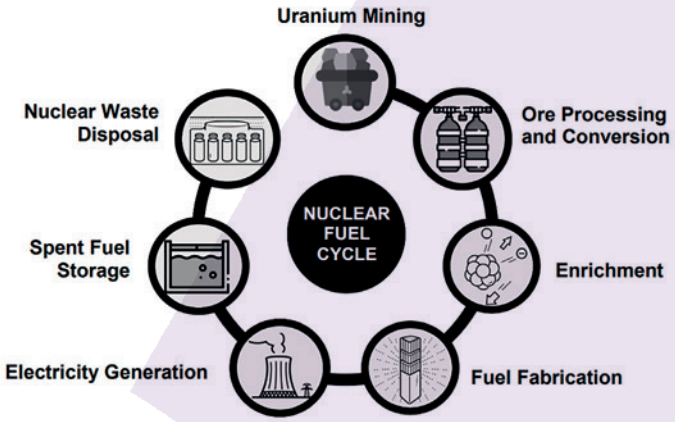


Figure 1. Overview of the Nuclear Fuel Cycle – Civil Nuclear Cyber Security Strategy 2022 [4]

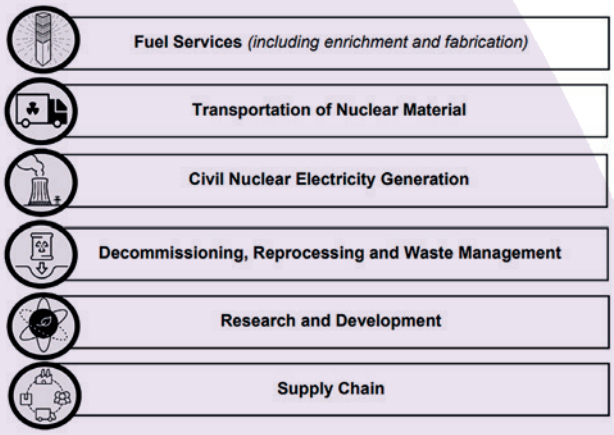


Figure 2. Civil Nuclear Sub-Sectors – Civil Nuclear Cyber Security Strategy 2022 [4]

- *Appropriately prioritise cyber security as part of a holistic risk management approach, underpinned by a common risk understanding, and outcome-focused regulation.*
- *Take proactive action to mitigate cyber risks in the face of evolving threats, legacy challenges and adoption of new technologies.*
- *Enhance resilience by preparing for, and responding collaboratively to cyber incidents, minimising impacts and recovery time.*
- *Collaborate to increase cyber maturity, developing cyber skills and promoting a positive security culture.*

Resilience and Strategy

Organisations are now striving for cyber resilience, not just protection, with strategies that ensure durability and the opportunities it can provide as a business enabler. The World Economic Forum (WEF) distinguishes cyber resilience from cyber security, with a more strategic, long-term outlook, driven by leaders that recognise the importance of risk mitigation and proactive risk management. Organisational leaders that set the strategy are ultimately responsible and are increasingly being held accountable for cyber resilience.[6]

The cyber-resilient organisation brings together the capabilities of cyber security, business continuity and enterprise resilience. It embeds security across the business ecosystem and applies fluid security strategies to respond quickly to threats, so it can minimise the damage and continue to operate under attack. As a result, the cyber resilient organisation can introduce innovation and operating models securely across the entire value chain, strengthening trust and instilling confidence.

The cyber security strategy provides objectives for an organisation's desired future security state and is integrated with the business strategy. This necessitates an understanding of the current state, with the strategy setting the course for achieving the desired future state within a defined period.

A cyber resilience strategy requires:

- An understanding of organisational risk.
- Activities to secure personnel and systems to prevent and resist cyber attacks.
- Preparation to ensure sufficient resilience in the event of a cyber attack, to minimise the impact and enable recovery.

Safety and Security

Nuclear security is not a subset of nuclear safety, and so delivering effective nuclear safety will not necessarily also result in effective nuclear security. Both are interconnected, yet safety and security engineering disciplines are independent domains. It cannot be assumed that obscure, bespoke systems or air gaps can prevent attacks. Similar challenges have been observed in rail safety, with security guidance for safety engineers and managers published by the Centre for the Protection of National Infrastructure (now the National Protective Security Authority). Convergence has been driven through common technologies, platforms, and networking, where safe operation of complex systems requires appropriate security. The two disciplines may also conflict, creating new functionality, vulnerabilities and hazards that may require additional mitigations to reduce safety and security risk in the provision of critical services. [7, 8] ▷

Colonial Pipeline disruption

Darkside ransomware targets critical infrastructure shutting down US petroleum pipeline causing international disruption and panic buying.

DarkSide ransomware attack impacted IT systems, however OT systems controlling the pipeline were shut down as a precaution. This interrupted the supply of 2.5 million barrels of aviation fuel, diesel, and petroleum daily across the entire US East Coast. The ransomware gang used remote access account credentials available on the dark web. Most of the $5 million ransom was recovered by the FBI from the gang's affiliate which led to the collapse of the DarkSide brand. The incident caused operational disruption with international impacts upon aviation and panic buying of petroleum and lawsuits.

Lessons identified included account management governance failings, where a vulnerable virtual private network profile was not intended to be in use, facilitated initial the gang access. OT network protection can atrophy over time creating hyper-connectivity due to cloud resources, system integrators, original equipment vendors, personnel, and enterprise IT, However, some organisations' IT and OT systems have tightly coupled dependencies, where segregation can be difficult to implement. Crown jewels protection is paramount, along with gaining visibility into OT networks with traffic monitoring and addressing insecure connectivity. Ensuring critical OT systems backups and incident response plans are in place and exercised is essential given the increasing threat of ransomware. [10, 25, 26, 27, 28, 29, 30]

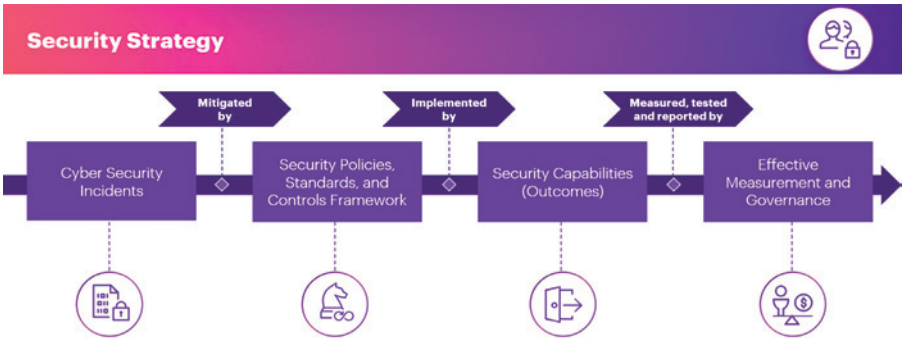


Figure 3. Cyber security strategy implementation

Governance shortcomings may impact the individual too, especially where OT cyber risks could lead to physical harm.

Widely published incidents across industrial sectors have demonstrated siloed approaches, focused on IT security, and omitting Operational Technology (OT) in particular, which expose potentially vulnerable systems. The IET Code of Practice: Cyber Security and Safety addresses this convergence and the necessity to integrate safety assurance and cyber security.[9] The publication also considers where there may be tensions between safety and security requirements, such as creating security induced safety hazards (e.g. inability to logon and access a safety system using shared accounts), and issues with estimating static safety risks, whilst considering the rapidly changing security environment, with dynamic threats and emerging vulnerabilities.

Importance of Strategy

Organisations pursuing cyber resilience require their senior stakeholders to proactively manage cyber risk, alongside other enterprise risks. Leaders set the organisational intent and describe outcomes to be delivered in the strategy. The strategy documents decisions and is used to control implementation and progress, whilst ensuring it aligns with the need of the organisation's business strategy.

A resilience focused strategy enables organisations to take advantage of digitisation and technological change, with an approach that enables the business and provides a source of competitive advantage, whilst maintaining value. Cyber security strategy alignment with business priorities ensures the resulting outcomes are proportionate to the risk faced by the business. The strategy quantifies organisational cyber risk appetite and tolerance. It will also help to identify threats to the organisation. Using recognised cyber frameworks will assist in the application of relevant good practice and meeting sector baselines. As such, it is also a regulatory requirement for dutyholders, being critical to effective implementation (Figure 3).

Security Strategy Principles

When assisting organisations in the implementation of their cyber resilience programmes, Accenture's approach uses the following guiding principles:

- **Business-centric**. Ensure cyber resilience is driven by business and organisational priorities. Accenture research showed this was a key differentiator of cyber resilient organisations, with significant financial advantages.
- **Enterprise-wide**. Cyber is an enterprise level issue, to be treated in a similar manner to other organisational risks. It isn't just an IT, Operational Technology, or a technology issue. It is an operating environment with risk, in the same way operations occur in a physical environment, where physical risks manifest.
- **Exposure focused**. The need to focus beyond compliance requirements to address actual exposure to be cyber resilient.
- **Extended ecosystem coverage**. Be responsible for the extended eco-system, not just the immediate supply-chain. Recent events have demonstrated systemic risks flow from the complex nature of digital systems and the interconnectivity with other systems and organisations. The Colonial Pipeline, Solarwinds and NotPetya incidents illustrate systemic risks. [10, 11, 12]
- **Agile**. Seek to build cyber security organisations that can evolve and grow along with the business.
- **Technology enabled**. Create a cyber resilient organisation that is technology enabled, not just full of technology. The security strategy should be technology agnostic, focusing on the desired outcomes, whilst providing flexibility to keep pace with technological change.

The cyber resilience strategy needs to align with the business strategy and its timeframe. Shorter than 2-3 years is fundamentally operational planning, which is not strategic.

Nation State Destructive Malware Disrupts Shipping Operations

Collateral damage from nation state cyber operations impacts global shipping operations raise company extinction concerns

The NotPetya malware infected almost 50,000 end-user devices and thousands of servers at the international shipping company Maersk and affected many other organisations. Maersk managed to rebuild all devices and applications within 2 weeks. The company reported approximately $300 million in losses, despite maintaining 95% of regular shipments. The Maersk Chairman, Jim Hagemann Snabe told the World Economic Forum in Davos they faced a company extinction event, and being average at cyber security is not enough. Maersk intends to use cyber security to create competitive advantage and treat these attacks as business risks, not technology concerns.

Lessons identified included, transparency, acknowledged as the principal lesson learnt, with support from clients and partners due to openness, and increased share value following the incident. Maersk recognised that most organisations are unlikely to be able to prevent a nation state attack, therefore the focus needs to be on recovery and prevention of extinction events. The extinction event approach uses consequence driven impact analysis, assuming the worst-case incident. This contrasts with traditional probability methods, which seek to identify both specific scenarios and their likelihood of occurrence. [12, 31, 32]

Governance and Leadership

The board and senior-level leadership are ultimately responsible for an organisation's cyber risk and resilience, a notion that is front and centre in ONR's outcome focused regulatory approach. The leadership holds primary accountability for discharging legal, regulatory, and mandatory requirements. As such, governance shortcomings may impact the individual too, especially where OT cyber risks could lead to physical harm. The leadership team must be aware of their role and responsibilities. All staff must understand their responsibilities for security and cyber resilience. It is essential that the leadership sets the tone for fostering and maintaining the organisational security culture, including managing cyber risk with safety.

The governance function establishes and maintains the organisational framework, with supporting process to ensure the security programme aligns with organisational goals and objectives. Accenture research revealed cyber security stimulates enterprise reinvention, driving business resilience, with a stronger alignment between cyber security practices and the business strategy achieving better outcomes (Figure 3). [13, 14]

An outcome-based approach, such as the Office for Nuclear Regulation's Security Assessment Principles and the National Cyber Security Centre's Cyber Assessment Framework (CAF) places the onus upon boards to manage risk and apply suitable judgement to achieve specified outcomes. Combining an outcome focus with risk management and the application of recognised cyber security frameworks provides greater business resilience and benefits over just chasing compliance. Implementation experiences demonstrate improved risk understanding, identifying strengths and areas for improvement, informed risk tolerance and prioritising security remediation, facilitating resource allocation and security budget setting. [15, 16]

Good governance should ensure accountability for decisions, their implementation, and the measurement of progress with key performance indicators. These will enable course corrections and the provision of feedback to senior stakeholders. An organisational wide governance structure and cyber security strategy will support the delivery of cyber resilience and demonstrate due care and diligence.

Cyber resilience and effective cyber risk management are critical challenges for many organisations. The consequences of poor security strategy can lead to reputational damage, loss in shareholder value, safety incidents and governance issues. Boards often say they lack both tools and competencies to manage cyber risks in the same way they approach other risks. Cyber security vocabulary is frequently a challenge in developing mutual understanding between boards and specialists. Ensuring a common frame of reference, with case studies or stories can help. Raising cyber security competency, with access to specialist expertise, will help to develop senior stakeholder's knowledge, ensuring effective oversight.

Accenture research identified four levels of cyber resilience (Figure 4). The Cyber Champions, organisations that strike a balance, not only excelling at cyber resilience, but also aligning with the business strategy to achieve better business outcomes. They are successful in at least three out of four cyber resilience performance criteria, better at stopping attacks, finding, and fixing breaches faster and reducing their impact. [13]

Risk Management

Senior stakeholders set the desired priorities, goals and outcomes by managing risk and determining the level of acceptable risk or risk tolerance. The acceptable risk is the level of risk the organisation will bear after risk measures have been put in place. Expressing risk appetite in financial terms will inform decision making. Risk tolerance is more granular, focused on specific risks, and how the organisation ▷

Disregarding Probability in Cyber Security Assessment to Address the Most Severe Outcomes

The US Idaho National Laboratory (INL) has developed a framework to secure critical infrastructure with the overriding assumption that should it be targeted by a skilled and determined adversary, the organisation's networks will be penetrated. [33] Thinking like an adversary provides all stakeholders (asset owners, operators, and suppliers) with a methodology to move beyond traditional security focused areas to evaluate an organisation's entire operations to secure the most essential operations, processes and technology. The framework expands on traditional assessments so that vulnerabilities are not just technically assessed, but also how they might be exploited to impact the entire organisation's operations and processes.

The INL approach take a four-step process:

1. Consequence prioritisation: Focus risk management to select mission/critical operations that must not fail and associated attack scenarios that could impact them.
2. System of Systems Analysis: Gathers information to identify systematic interdependencies between critical processes, defences, and enabling or dependent components.
3. Consequence-based targeting: Adversary's path determination to achieve the highest impact effects, location to execute an attack, and the information required.
4. Mitigations and protections: Digital attack pathway removal or disruption.

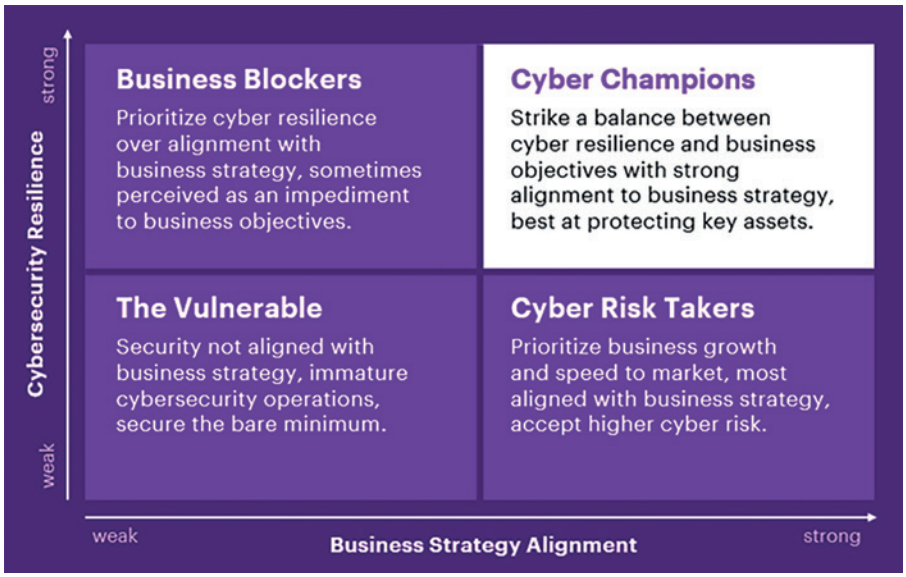


Figure 4. Four levels of cyber resilience – Accenture State of Cybersecurity Resilience 2021 [13]

Figure 5. Risk management presentation to the board – examples

would cope if they deviated from the risk appetite. Stakeholders should regularly ensure organisational risk tolerance is consistent with the organisational risk appetite. An example of risk identification and assessment is shown in Figure 5.

When undertaking risk assessments, an organisation will identify, assess, and seek to understand security risks to critical systems, both in IT and OT. It is important to assess the methods that might be used by attackers. The MITRE ATT&CK® knowledgebase illustrates adversary tactics and techniques, from initial access through to impact in IT and OT environments.

The differing impacts are illustrated in Tables 1 & 2. The recently revised NIST SP 800-82r3 Guide to Operational Technology Security provides comprehensive guidance, whilst introducing readers to OT's unique characteristics. [17, 18]

Organisations then need to put measures in place to specifically defend against these and monitor progress with suitable key performance indicators (KPIs) to measure risk reduction. An example would be privileged account management, and relevant KPIs, including the number of users, the number of newly created users, and number of roles relative to number of departments.

The risk management topic also includes the organisational approach to risk, including governance, and management accountability for reporting cyber risk to the board. This forms the foundation to the governance operating model, which brings the security strategy and

Cyber Attacks Have Already Targeted Hazardous Processes

The Triton (also known as Trisis or Hatman) malware specifically targeted Schneider Electric's Triconex Safety Instrumented System with the intent to manipulate industrial control systems in a Middle Eastern petrochemical plant. Safety systems are used to protect systems and provide emergency shutdown of hazardous processes. Industrial safety systems run independently from the main control system to monitor and prevent potentially dangerous conditions. The malware was designed to compromise the system and manipulate the controller to override the safety system and cause a failure that could lead to a dangerous physical incident. [34, 35, 36, 37]

MITRE ATT&CK® ENTERPRISE IMPACT
Account AccessRemoval
Data Destruction
Data Encryption for Impact
Data Manipulation
Defacement
Disk Wipe
Endpoint Denial of Service
Firmware Corruption
Inhibit System Recovery
Resource Hijacking
Service Stop System
Shutdown/Reboot

Table 1. MITRE ATT&CK ® Enterprise Impact
Source: https://attack.mitre.org/matrices/enterprise/

MITRE ATT&CK® ICS IMPACT
Damage to Property
Denial of Control
Denial of View
Loss of Availability
Loss of Control
Loss of Productivity and Revenue
Loss of Protection
Loss of Safety
Loss of View
Manipulation of Control
Manipulation of View
Theft of Operational Information

Table 2. MITRE ATT&CK ® ICS Impact
Source: https://attack.mitre.org/matrices/ics/

Nuclear security is not a subset of nuclear safety, and so delivering effective nuclear safety will not necessarily also result in effective nuclear security.

business objectives together and is used to operationalise the governance programme to monitor and support cyber security initiatives. The implementation should provide end to end traceability of cyber security, business risk and threat management through defined governance, policy, and control monitoring.

Security Strategy Components

Outlining the purpose, vision and mission are the starting points for the cyber security strategy. These capture how security will be an enabler to the organisation, unpinning strategic business objectives. An end-to-end understanding of how the organisation delivers value is an important lens when considering the risk and threats faced. This process will identify how various functions support activities in the value chain, and shape the security strategy, and the plan to address risks and threats.

The security concerns, such as Confidentiality, Integrity, Availability or Safety will drive security and their emphasis will differ across the value chain and their environments. OT requires different security approaches due to control systems and their physical interaction. An understanding of the degree of risk/consequence across the value chain is necessary to make informed decisions regarding security investments and strategic next steps. Thus, planning to protect what is important, often referred to as 'identifying the crown jewels.'

Cyber security frameworks can be used as a systematic approach to managing cyber risk. The functions shown in Figure 6 are regarded as the essential pillars of a holistic cyber security programme:

- **Identify** – understanding and managing risk to systems, people, assets, data, and capabilities.
- **Protect** – implementation of safeguards and limiting the impact of cyber security incidents.
- **Detect** – activities to identify and to permit timely discovery a cyber security event.
- **Respond** – actions taken when a cyber security incident is detected, to contain the impact of the event.
- **Recover** – resilience and restoration planning and activities for the timely recovery of capabilities or services impaired following a cyber security incident.

Frameworks can be used to define cyber resilience functions, with a collection of lower level contributing cyber security and resilience outcomes. These are illustrated using the US National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF), which is mapped to the ONR Security and Assessment Principles (SyAPs) in Figure 4. [19, 15]

Fundamental Security Principle 7 (FSyP7) within ONR's SyAPs, states dutyholders must implement and maintain effective cyber security and information assurance arrangements to protect Sensitive Nuclear Information (SNI) and technology. SyAPs are also outcome focused and used by ONR to assess dutyholder's security arrangements. [20]

The National Cyber Security Centre (NCSC) guidance, known as the Cyber Assessment Framework (CAF) has deliberate similarities with the NIST CSF. Both the NIST CSF and NCSC CAF refer to relevant good practice, including ISO/IEC 27001/27002 standard series and IEC 62443 series for control systems or Operational Technology (OT). ▷

OT and IT Have Different Security Requirements

OT

- *Limited data capacity and computing;*
- *Safety operations are critical;*
- *High availability & integrity are vital, confidentiality is less stringent;*
- *Critical operations/systems at network edge with humans at the centre;*
- *Long life (often decades) resulting in legacy, unsupported infrastructure;*
- *Essential equipment and operations remotely deployed network edge;*
- *Slow response to threats-rapid patching might be impossible due to outages.*

IT

- *High data capacity and computing power;*
- *Few safety critical operations;*
- *Confidentiality & integrity are vital while availability is important;*
- *Critical operation and systems are at the network centre, with human users at the edge;*
- *Continuous equipment upgrades with short life cycles;*
- *Essential equipment and operations concentrated at network centre;*
- *Rapid response to threats, patching forced reboots are acceptable.*

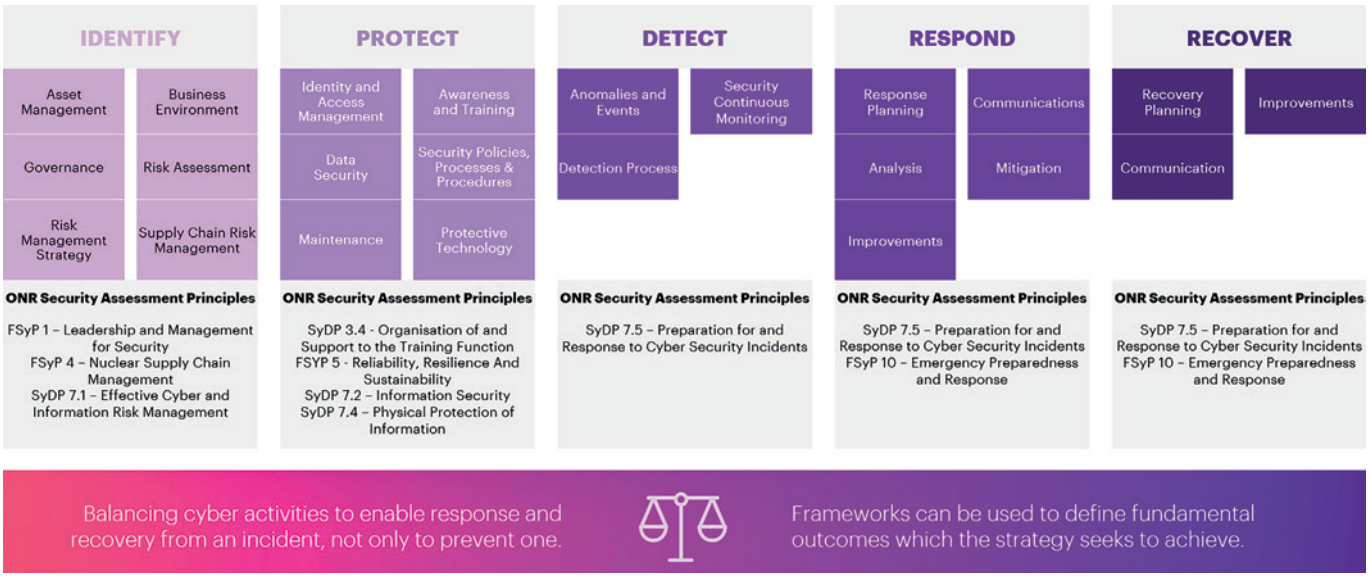


Figure 6. Relevant good practice: NIST CSF mapped to ONR's SyAPs

The NIST CSF and NCSC CAF both provide a common language and mechanism to describe an organisation's current state and future target states. They also help to identify and prioritise improvements, measure progress and communicate cyber security risks. The recent NIST framework developments in the CSF 2.0 are especially relevant, including the addition of the Govern function, establish and monitor cybersecurity risk management, strategy and policy. There is also increased emphasis upon supply chain management and secure software development. [21]

Security Culture

Convergence has increased the need to manage cyber security, and develop a security-informed approach to safety, where security considerations are integrated into the management of safety risks. Security threats that impact safety must be considered to ensure a security minded engineering approach, which addresses security threats and vulnerabilities throughout the lifecycle.

Embedding a proactive cyber security culture and mindset is essential to enabling the digital enterprise. A positive security culture will mitigate security risks where technology alone is insufficient. Human factors remains the principal source of cyber security breaches, due to lack of awareness and suitable training. The senior leadership needs to define, demonstrate, and inspire a positive security culture and encourage collaboration across disciplines. [22]

Organisations should focus on the following areas to build a proactive cyber security culture:

- Strategic executive alignment is critical to build a cohesive ownership of cyber security across IT and OT and address potentially incompatible approaches to addressing cyber risk.
- Upskilling of IT & OT cyber security "joint taskforce" professionals with the right skills to enable and sustain cyber security across the organisation.
- Establishing incentives and disincentive policies to promote and enforce cyber resilient behaviours across the organisation.
- Implement continuous, interactive and human centred awareness and learning programme to build user alertness including new joiners and third parties.
- Driven by data analytics, predictive models as opposed to traditional approaches to measure behavioural change against vulnerabilities.
- Leaders to lead by example and inspire their teams to demonstrate cyber resilient behaviours.

Clear expectations should be set for staff behaviour, and an acceptance that incidents will arise, with staff encouraged to report issues so they can be rectified swiftly, without threat of blame or criticism. The security culture is the foundation of daily life in the organisation, where poor cyber security is simply not acceptable.

- Is there an open approach to assess security in no-blame manner?
- What level of training and awareness do employees have?
- How could employees or an insider cause an incident, intentionally or by accident?
- Do key stakeholders have a thorough understanding of the insider threat programme and the risks faced by the organisation? [23]
- Does the culture enable cyber resilience to be used as a justification?

Conclusions

It is important for the strategy scope to cover the entire cyber environment, including information systems, control systems, safety systems, security systems, building management systems and Internet of Things (IoT Sensors/Actuators). An integrated approach must incorporate security into safety cases to address security issues, technology convergence and deal with the potential tensions between safety and security that may arise. This necessitates creating a common understanding across safety and security disciplines, emphasising the importance of leadership and a positive security culture. Leadership teams have a legal responsibility to manage safety and security risks, and shortcomings will have inevitable consequences for accountable individuals.

Acknowledgements

It is acknowledged that the briefing materials this article is based upon were commissioned by the Office for Nuclear Regulation in support of the 2022 Civil Nuclear Cyber Security Strategy.

The briefings, whitepaper and subsequent dissemination activities have been recognised with ONR and Accenture shortlisted as finalists for both the Security and Cyber Outstanding Security Performance Awards (OSPAs). •

Operational Technology Challenges

A cyber-attack targeting OT, leading to a prolonged loss of the electricity grid, loss of logistic capabilities, or platforms, could have severe consequences, including the potential for loss of life. As such, a cyber-attack could have comparable effects to a physical attack.

Costs reduction and improved efficiency drive adoption of digital solutions but security is often overlooked. There is a shortage of experienced personnel with converged IT/OT security expertise. OT is found in complex environments, with overlapping green and brownfield technologies which can lead to complex integration, visibility, and vulnerability issues. Increasing connectivity potentially expands the attack surface.

Richard Piggin *has an Engineering Doctorate (EngD) from the University of Warwick, (industrial automation networking), and has recently completed the Cyberspace Operations Postgraduate Diploma at Cranfield. He is a Chartered Engineer (MIET & MBCS). He was a co-instigator and contributor for the IET Code of Practice for Security and Safety. Richard recently joined ONR to undertake a cyber security and information assurance regulatory role. Richard focused on critical infrastructure cyber security consultancy with Accenture, when these briefings were undertaken and this article was produced. He has also worked with control system vendors in cyber security, industrial networking, and safety technology. His experience includes delivering innovation programmes and leading projects in the aviation, nuclear, oil & gas, electricity, water, chemicals, transport, medical, metals, automotive, manufacturing, government and security sectors. He continues to raise awareness of critical infrastructure security, having published over 100 papers.*

REFERENCES

1. ONR, Chief Nuclear Inspector's Annual Report on Great Britain's Nuclear Industry 2022/23, 2023, p. 12 https://www.onr.org.uk/documents/2023/cni-annual-report-2023.pdf
2. Piggin, R. Leading cyber security in the UK civil nuclear sector, ITNOW, Volume 65, Issue 4, Winter 2023 https://doi.org/10.1093/itnow/bwad129
3. ONR, Chief Nuclear Inspector's Annual Report on Great Britain's Nuclear Industry 2022/23, 2023, pp 12-13 https://www.onr.org.uk/documents/2023/cni-annual-report-2023.pdf
4. DESNZ (formerly BEIS), Civil Nuclear Cyber Security Strategy 2022, 2022 https://www.gov.uk/government/publications/civil-nuclear-cyber-security-strategy-2022
5. WEF, Global Risks Report 2023, 2023, p. 42 https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf
6. WEF, Principles for Board Governance of Cyber Risk, 2021 https://www.weforum.org/reports/principles-for-board-governance-of-cyber-risk
7. CPNI, Rail Code of Practice For Security-Informed Safety, 2022 https://www.npsa.gov.uk/system/files/documents/rail-code-practice-security-informed-safety.pdf
8. P. Litherland ; R. Orr ; R. Piggin, Cyber security of operational technology: understanding differences and achieving balance between nuclear safety and nuclear security, 11th International Conference on System Safety and Cyber-Security, 2016NCSC, Cyber Security Body Of Knowledge (CyBOK), 2021 https://www.cybok.org/media/downloads/Introduction_v1.1.0.pdf
9. IET, Code of Practice: Cyber Security and Safety, 2021 https://electrical.theiet.org/guidance-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-and-safety/
10. US DOE, Colonial Pipeline Cyber Incident, 2021 ttps://www.energy.gov/ceser/colonial-pipeline-cyber-incident
11. FCDO, Russia: UK exposes Russian involvement in SolarWinds cyber compromise, 2021 https://www.gov.uk/government/news/russia-uk-exposes-russian-involvement-in-solarwinds-cyber-compromise
12. Wired, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, 2018 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
13. Accenture, State of Cybersecurity Resilience 2021, 2021 https://www.accenture.com/gb-en/insights/security/invest-cyber-resilience
14. Accenture, The Cyber-Resilient CEO, 2003 https://www.accenture.com/content/dam/accenture/final/accenture-com/document-2/Accenture-The-Cyber-Resilient-CEO-Final.pdf
15. ONR, Security Assessment Principles (SyAPs) Version 1, 2022 https://www.onr.org.uk/syaps/
16. NCSC, CAF guidance version 3.1, 2022 https://www.ncsc.gov.uk/collection/caf
17. MITRE, ATT&CK® Matrix for ICS, 2023 https://attack.mitre.org/matrices/ics/
18. NIST, NIST SP 800-82r3 Guide to Operational Technology (OT) Security, 2023 https://doi.org/10.6028/NIST.SP.800-82r3
19. NIST, Cybersecurity Framework, 2024 https://www.nist.gov/cyberframework
20. ONR, Security Assessment Principles for the Civil Nuclear Industry. 2022 Edition Version 1, 2022, p. 22 https://www.onr.org.uk/syaps/security-assessment-principles.pdf
21. NIST, The NIST Cybersecurity Framework 2.0, 2024 https://doi.org/10.6028/NIST.CSWP.29
22. WEF, Global Risks Report 2022, 2022, p. 52 https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
23. NPSA, Reducing Insider Risk, 2023 https://www.npsa.gov.uk/reducing-insider-risk
24. HMG, National Cyber Strategy 2022, 2022 https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022
25. Accenture, Securing the T&D network of the future – The path forward: operational security in utility transmission & distribution, 2022, pp. 12-13
26. WEF, Global Risks Report 2022, 2022, pp. 47-48 https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
27. Dragos, Recommendations Following the Colonial Pipeline Cyber Attack, 2021 https://www.dragos.com/blog/industry-news/recommendations-following-the-colonial-pipeline-cyber-attack/
28. Blount, J., Testimony of Joseph Blount, President and Chief Executive Officer Colonial Pipeline Company. Senate Committee on Homeland Security & Governmental Affairs, 8 June 2021, p. 4 https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Testimony-Blount-2021-06-08.pdf
29. NCSC, NCA, Ransomware, extortion and the cyber crime ecosystem, 2023 p. 8 https://www.ncsc.gov.uk/pdfs/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem.pdf
30. CISA, #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability, 2023 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a
31. The Register, IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation blitz, 2018 https://www.theregister.com/2018/01/25/after_notpetya_maersk_replaced_everything/
32. CSO, Rebuilding after NotPetya: How Maersk moved forward, 2019 https://www.csoonline.com/article/567845/rebuilding-after-notpetya-how-maersk-moved-forward.html https://digital-library.theiet.org/content/conferences/10.1049/cp.2016.0856
33. INL, Consequence-driven Cyber-informed Engineering, 2023 https://inl.gov/content/uploads/2023/06/Consequence-driven-Cyber-informed-Engineering.pdf
34. Wired, Unprecedented Malware Targets Industrial Safety Systems in the Middle East, 2017 https://www.wired.com/story/triton-malware-targets-industrial-safety-systems-in-the-middle-east/
35. Dragos, TRISIS Malware: Analysis of Safety System Targeted Malware, 2017 https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf
36. Wired, Menacing Malware Shows the Dangers of Industrial System Sabotage, 2018 https://www.wired.com/story/triton-malware-dangers-industrial-system-sabotage/
37. Darkreading, Triton/Trisis Attack Was More Widespread Than Publicly Known, 2019 https://www.darkreading.com/attacks-breaches/triton-trisis-attack-was-more-widespread-than-publicly-known

The senior leadership needs to define, demonstrate, and inspire a positive security culture and encourage collaboration across disciplines.

GET Involved

Calling all Book Reviewers, Product Reviewers, Bloggers and Evangelists!

The world of Digital Forensics and Digital Investigations is ever expanding, and we are now way beyond the standard Mobile Phone, Tablet and Hard Disk analysis. Whilst these devices continue to develop, we will of course need to continue to research and develop ways to forensically examine them as they develop new technologies for the devices, apply new security technology or new applications are developed that may hold forensic artefacts useful to an investigation.

Technology is now all pervasive and impacts every aspect of our lives, this means that digital investigations of the future will include a wider and more diverse range of technologies, there will be an ever-increasing need for new technology to assist in the investigations and the investigators will require new and additional knowledge and skills in order to carry out the investigations. Along with all this, new technological standards will need to be understood and new standards associated with the deployment of new technologies will need to be written.

Whether the Digital Investigation is in support of a larger criminal investigation, the investigation of a data breach, a cyber-attack with real world consequences (e.g. an attack on a utility company infrastructure that caused a regional outage), a health and safety investigation related to an industrial accident, any form of transport incident investigation especially where increasing degrees of autonomy are encountered; digital investigators need to know how to forensically investigate this emerging (some may say already arrived) increasingly technological world.

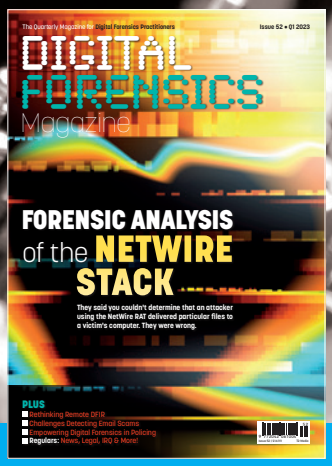
This landscape increases in complexity as we interconnect systems to become system of systems where the number of systems that are interconnected may be significant in terms of number and diversity. The ever increasingly connected supply chains, the use of AI to increase decision making resulting in greater automation and the use of QUANTUM technologies giving rise to better sensing technologies and speed of computation all need to be factored into future Digital Investigations. On top of this we have greater use of SPECTRUM in our digital communications, with 5G & 6G set to revolutionise the number of devices that maybe connected in a non-tethered manner. The developments of the emerging technologies to be used in Space both on board spacecraft and from a world sensing perspective will also have an impact on the way that we carry out investigations as many may have artifacts of interest to a digital investigator as they seek to establish the sequence of events that occurred during a specified timeline.

Here at *DFM*, we are looking to ensure that we can continue to bring you articles from both the research and the practitioner community. So, if you or your organisation has an article, or an idea for an article, that you believe is relevant to the world of Digital Forensic Investigations we want to hear from you. You can either contact us directly by writing to the Editor at editor@digitalforensicsmagazine.com or by submitting an abstract via the website. We especially would like to hear from those Universities who are actively educating and researching the digital world as we often find that good student projects are worthy of being published but are rarely seen outside of the University.

This does not mean that we are not interested in real world experience of what is happening now, indeed practical case studies are of great interest to the magazine and readership, so if anyone had a real-world investigation that they would like to share, we would also like to hear from you. We are also interested in anyone who might like to become a regular blogger for the DFM Blog, especially where the blog is about thought leadership and not just an opinion of the latest news. The latter is still important; however, we are trying to get people to think about the future rather than just the here and now.

So, if you feel you have an idea for an article or an example from the real world, we want to hear from you. Here is but a sample of articles likely to appear in future issues. •

BACK Issues



Issue 50
Q3 2022

- Romance Fraud & The Elderly
- Apparel Industry Fraud Update
- TikTok Cybersecurity and US-China Tensions Part 3
- Industrial Internet of Things Security
- Faster Payments Fraud
- Raising the Bar for Digital Evidence Collection

Issue 51
Q4 2022

- Finding the Needle in the Lawful Intercept Haystack
- Dealing with DSARs
- Preparing for PCI DSS v4.0
- Justice Delayed Is Justice Denied
- Cyber Forensic Tool Machine Learning
- Meta Becomes Target of Litigation for Healthcare Privacy Violations

Issue 52
Q1 2023

ARSENAL FEATURE

- **Forensic Analysis of the NetWire Stack**
- Rethinking Remote DFIR
- Challenges Detecting Email Scams
- Empowering Digital Forensics in Policing
- The Collapse of FTX and Related Misbehaviour

Issue 53
Q2 2023

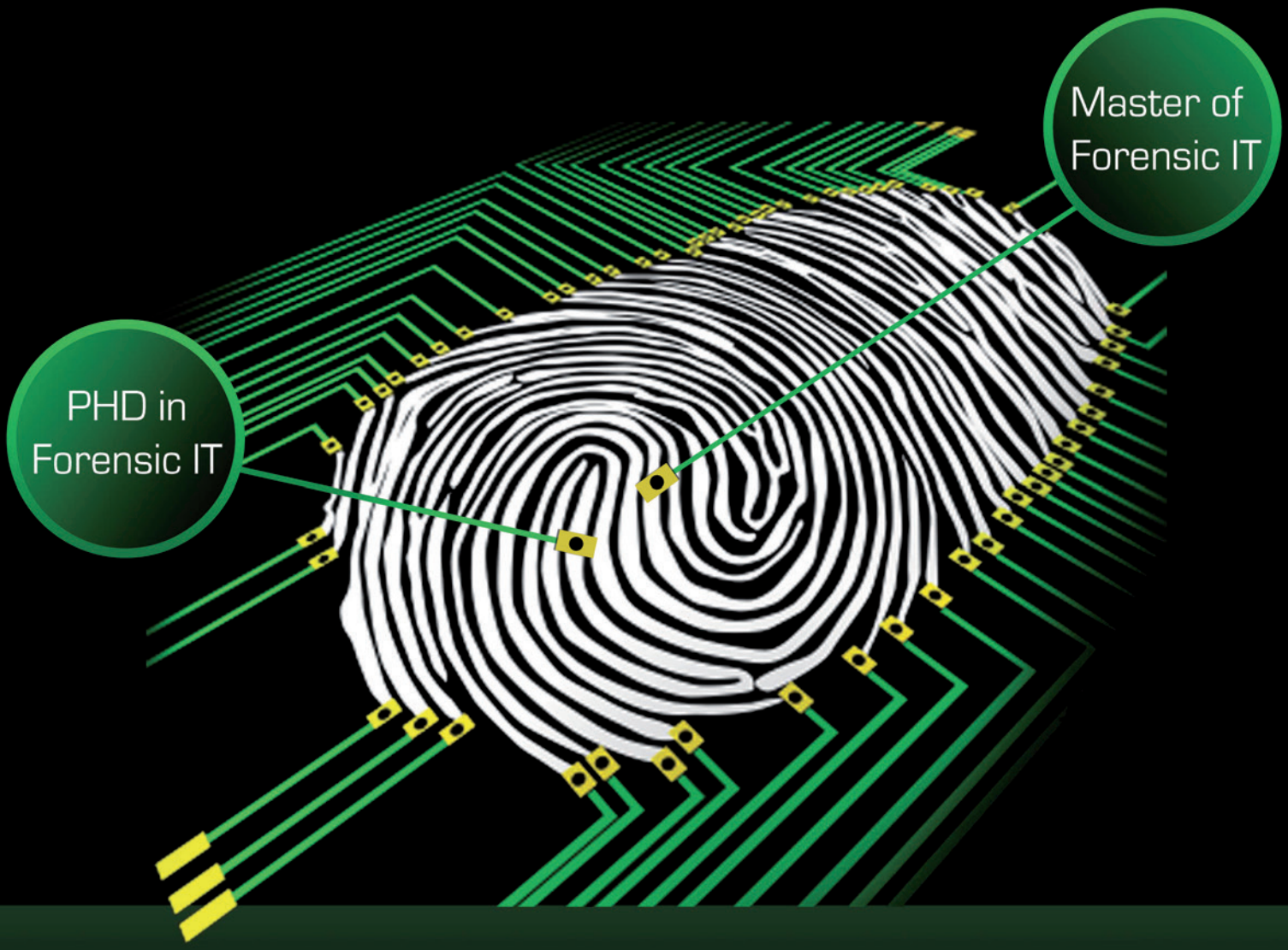
- Enhancing Access Controls with Artificial Intelligence
- The Role of AI in the Criminal Justice System
- Unveiling the Origins of Artificial Intelligence
- WannaCry – Cybersecurity Vulnerabilities
- The History of The Cyber Scheme
- OpenAI and Microsoft

ORDER ONLINE

www.digitalforensicsmagazine.com

AUT
UNIVERSITY
AUCKLAND, NEW ZEALAND

The University for the changing world



DIGITAL FORENSIC RESEARCH

School of Computing and Mathematical Sciences Laboratories

www.aut.ac.nz

NEXT Issue

Here are some of the articles we are reviewing for future issues. If you have an idea for an article, contact us at 360@digitalforensicsmagazine.com or submit your abstract via the website.

Forensic Readiness

Why are companies not prepared enough for potential issues? How do you build a proactive approach to cyber and IR preparedness and how do you build the business case? With future legislation looking to make Forensic Readiness a legal requirement, Larry Gagnon looks at what is required.

How the Metaverse is Challenging Forensic Investigation

The Metaverse is a phenomenon that is rapidly evolving and taking shape as a services platform and mediating ecosystem for human computer interaction. It currently has an abstract and incoherent profile that challenges human imagination to visualise what is socially, technically, and commercially viable. Brian Cusack investigates.

Visualizing IoT/IIoT Data with Recharts and InfluxDB

IoT Data is harvested from a wide range of sensors on manufacturing infrastructure, weather stations, smart meters, cars, fridges and many other devices. All this data has to be processed in order to make one interpretable feed of data. This can help with reverse engineering and failure prediction. In this article we will be developing a visualization platform that will display disparate IoT data for further analysis.

Cracking the Complexity Conundrum of Forensic Investigations in the Digital Age

To understand and make sense of the future, sometimes it helps to look to the past. This can be especially illuminating when it comes to digital forensics given just how fast the consumer technology landscape can change in a relatively short period of time.

How to Mitigate the Cybersecurity Dangers Facing Forensic Investigators

This article will investigate the current dangers facing digital forensic investigators and law enforcement forces; how this trend has evolved in recent times and how it will likely continue to grow as we move into 2024. Why online investigators must be more vigilant than ever, with the avenues of attack now wider than ever for malicious groups. Practical tips to help investigators and law enforcement organisations remain secure in 2023 and beyond. How digital infrastructures within enforcement bodies have changed in recent years. Industry stats and figures.

Note: We may change the planned content of future issues without notice; inclusion here does not guarantee publication in the subsequent issue.

IRQ

Submitted, for your consideration (Part 3)

The story so far : In a parallel universe, *our hero, Alex (aka "The Prof") has developed a new technique for identifying people based on their DNA. A police inspector has asked if this could be used to assist with the investigation of a serial killer. The police contacted The Prof's University to set up a contract and asked for detail of their registration with the Scientific Evidence Regulator. The University's legal department is now involved, and worrying about insurance and dealing with complaints...*

"Sorry Alex, it's not good news. I've spoken to the insurers at length, and asked the VC's risk management committee what their view is. We're all agreed that the potential cost if this results in a complaint is probably too high - but it's worse than that. We could argue that it falls under the 'occasional' expert category, which allows unregistered and non-compliant experts to give evidence a couple of times a year, but the insurers really don't like the sound of that.

There's also a worry that it could open the floodgates to more work, if this method is as good as you think it is. If that happened, we'd be looking at setting up a whole new business unit just to process police cases. The recruitment alone would take six months, and then there's all the quality processes that need to be set up and the validation studies that you'd have to do, and the lab. and office space and all the other things we need in order to show compliance. We reckon we're looking at something like £100k, minimum, as an annual cost. Now, if we could guarantee it would bring in enough work to cover that, at least, we could look into it, but we just don't know yet. "

"I'm really sorry, but the system seems to have been accidentally designed to make it pretty much impossible to bring in any new techniques or labs."

John was in full flow, explaining the results of another two month's digging into the regulatory problems.

Alex frowned, this time, then spoke. *"So... If we can't do it ourselves, can we licence it to someone else and let them take the risk while we collect licence fees?"*

"Well, we did consider that, but if we're going to go down that route we need to get some patents in place so that we can enforce licences properly. We have a couple of concerns about that too. Firstly, you've published some of the results already so there may be problems actually getting the patents in the first place, and secondly there's the time. We're probably looking at a minimum of 2 years, even if there are no objections or claims of prior art. And that's just for this country. Worldwide could take even longer. "

"So..." began Alex, *"basically, we're screwed either way. If we go ahead without this SER stuff we could end up in court for other reasons, and if we try to do it in a compliant way it could all be too late."*

"That's about the size of it. I'm really sorry, but the system seems to have been accidentally designed to make it pretty much impossible to bring in any new techniques or labs. in a hurry.

We might have one bit of good news, though. OK - it's not exactly as headline grabbing as getting involved in murder investigations, but certainly potentially more lucrative. The Dubai Jockey Club has been in touch to ask if your method might be able to help them with some questions about thoroughbred bloodlines. They're quoting some astronomical figures as sponsorship for setting up a lab. to help with that. The VC's really quite excited about the prospect of a new research centre..."

All persons and events in this story are fictitious. Any similarity to real persons, living or dead, or events is entirely coincidental. •

Angus Marshall *is an independent digital forensics practitioner, author and researcher, currently working on the 'fitness for purpose' challenge. In a past life he was an academic course leader in Digital Forensics and Forensic Computing and still retains strong links with academia, professional bodies and regulators. He can be contacted through his company, n-gate ltd. (http://www.n-gate.net).*

Accelerate digital forensics analysis with research and development.

Investigators may be overwhelmed by the complexity and volume of evidence found on computers, cell phones, and other devices. Departments may be unable to keep up with rapidly evolving technologies and evidence they produce.

That's where we come in.

The National Institute of Justice (NIJ) — the research and development arm of the U.S. Department of Justice — funds projects that move digital forensics forward with new methods and tools that collect and process digital evidence.

Our resources and funding strengthen the quality and practice of digital forensics through research and development, testing and evaluation, technology, and information exchange.

NIJ | National Institute of Justice

STRENGTHEN SCIENCE. ADVANCE JUSTICE.

Scan to learn about NIJ's resources.

Photo credit: Microgen/Shutterstock and Hans-Joachim Roy/Shutterstock

THE CYBER **SCHEME**

Qualify with us to join the best in the business.

The Cyber Scheme provides the highest standard of Government approved examinations available, essential for technical consultants wishing to gain NCSC CHECK status.

Additionally we are here to support, educate and recruit a new generation of talent through our in-house training facilities, addressing the current skills gap and ensuring that a robust cyber industry can protect the UK into the future.

As a not-for-profit organisation we are also committed to helping our charity partners educate the wider community through our innovative sponsorship scheme, providing support and education as well as developing training for those from a non-academic background interested in a career in this exciting industry.

Contact us today if you would like to know more about our industry-leading assessments, training and sponsorship opportunities.

"This was my first interaction with The Cyber Scheme and it was a very positive experience. The booking was easy, the communication from the staff was great and any queries were quickly answered and resolved.

On the day the assessors were very clear on the rules, scoping and expectations. The scoping and interview aspects were handled really well, and it is reassuring to know that the assessors understand what is required and have a higher level of technical knowledge than the candidates."

Member of

UK CYBER SECURITY COUNCIL

The Cyber Scheme
Eagle Tower, Montpellier Drive
Cheltenham GL50 1TA
admin@thecyberscheme.org
www.thecyberscheme.org

The Cyber Scheme is a member of the Cyber Security Council and will ensure the standards we develop are fully aligned with the Council and the wider aims of the UK Government. Our mission is consistent with the UK Government's National Cyber Strategy 2022, focussing on building a resilient Digital UK.